COPYRIGHT RESTRICTIONS

EXCEPTIONS from the COPYRIGHT RESTRICTIONS

Exclusively the students registered for the course of Dr. Tibor Tuzson have the right to make a 50% sized, or smaler copy for their personal study.

Nur die eingeschriebene Studenten/inen für die Vorlesung von Dr. Tibor Tuzson sind berechtigt für eigene Studium eine 50%, oder kleiner verkleinerte Kopie zu machen.

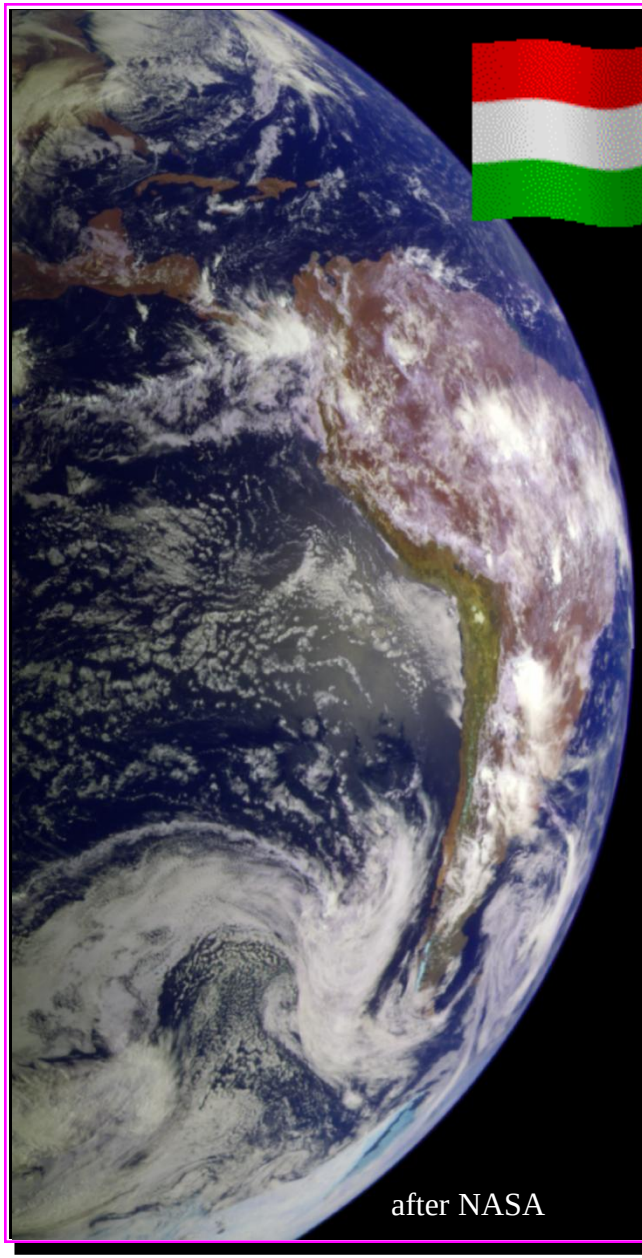
Kizárólag a Dr. Tuzson Tibor tanfolyamára beiratkozott hallgatók jogosultak saját tanulmányaikhoz egy darab, 50 %-ban, vagy még jobban kicsinyített másolatot készítésére.

DISCLAIMER

- **It was thoroughly checked, but it may contain yet errors. No liability is accepted.**
  Neither the author nor the teaching organization or institute provide any warranty, express or implied, for this teaching material.

- **Annak ellenére, hogy a szerző ismételt tüzetes szakmai vizsgálat tárgyává teszi a teljes oktatási anyagot, az még tartalmazhat hibákat vagy elírásokat. Ezekért a szerző, vagy az oktatási intézmény nem vállalhat semmiféle felelőséget vagy garanciát. Lényegében minden forrás megbízhatósága hasonló megkötésekkel korlátozott.**

Gregorian - Masters Of Chant: *Moment of Peace - interlude*



after NASA

BÁTHORY BRASSAI KONFERENCIA

ADABIZTONSÁG ÉS KRIPTOGRÁFIA

Dr. Tuzson Tibor
tuzsont@hdsnet.hu

templom és iskola

Reményik Sándor

Kolozsvár 1925

Ti nem akartok semmi rosszat,
Isten a tanútok reá.
De nincsen, aki köztetek
E szent harcot ne állaná.
Ehhez Isten mindannyitoknak
Vitathatatlan jogot ád:
Ne hagyjátok a templomot,
A templomot s az iskolát!

ADATBIZTONSÁG és KRIPTOGRÁFIA

BÁTGORY-BRASSAI KONFERENCIA, BBK

Balatonlelle 2011. Július 2.

Dr Tuzson Tibor

tuzson@mbit.hu

"Ha hajót akarsz építeni, ne azzal kezdd, hogy fát gyűjtesz, deszkákat vágsz és megszervezed a munkát, hanem keltsd fel az embereidben a vágyat a nagy, végtelen tenger iránt."

„Quand tu veux construire un bateau, ne commence pas par rassembler du bois, couper des planches et distribuer du travail, mais reveille au sein des hommes le desir de la mer grande et large."

Wenn du ein Schiff bauen willst, so trommle nicht Leute zusammen, um Holz zu beschaffen, Werkzeuge vorzubereiten, sondern wecke in ihnen die Sehnsucht nach dem endlosen, weiten Meer.

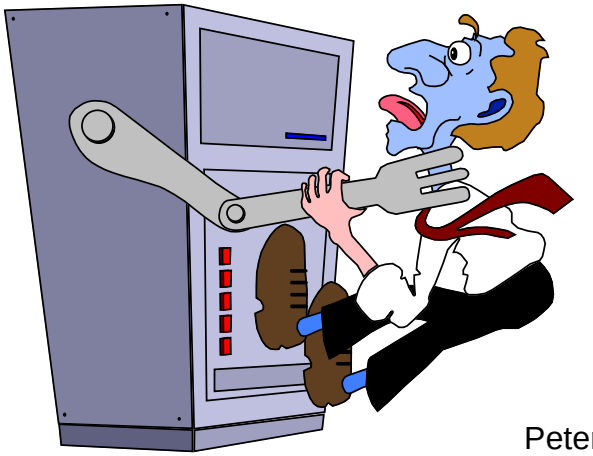
(Antoine de Saint-Exupéry)

After: Dr. Ronald Schnetzer:
Business Process Reengineering

LEGAL ISSUES

In God we trust.

All others we monitor.



NSA USA motto

Peter Gutmann: Cryptography and Data Security,
University of Auckland, New Zealand, Course Handout

Orosz népmese végződése (KGB módra)

Itt a vége,

Fuss el véle,

S ha nem hiszed,

Majd utánad járunk.

KRIPTOLÓGIA BEVEZETŐ

CRYPTOLOGY INTRODUCTION

KRYPTOLOGIE EINLEITUNG

„Ha azt hiszed, hogy a kriptográfia megoldja a problémádat, akkor vagy nem ismered a problémádat, vagy nem ismered a kriptográfiát."

Bruce Schneider

ADATREJTÉS MINT TUDOMÁNYÁG

KRIPTOLÓGIA:

Titkos ill. védett kommunikáció és adattárolás tudománya.
Csak az üzenet információ tartalmát rejti el, az üzenet létét nem. Két ága van:

- **KRIPTOGRÁFIA:** Azon algoritmikus módszerekkel és adatátviteli protokollokkal foglalkozik, amelyek biztosítják az üzenetek ill. tárolt információk **titkosságát, sértetlenségét** vagy **hitelességét**.
  - **kriptográfiai algoritmusok:** a rejtjelzést és visszafejtést lehetővé tevő matematikai ismeretek és (számítási) algoritmusok tudománya.
  - **kriptográfiai protokollok:** azon adatátviteli eljárások összessége amelyek biztosítják a rejtjelző kulcsok, valamint az átvitt, rejtjelzett adatok titkosságát, integritását, hitelességét és a rejtjelző rendszerek támadásokkal szembeni ellenállását.
- **KRIPTOANALIZIS:** a titok (üzenet, kulcs), általában illetéktelen megfejtésének, feltörésének tudománya.

STEGANOGRAFIA

A rejtett kommunikáció és adattárolás tudománya. Az üzenet létét is elrejti.

VÍZJELZÉS

A rejtett információ csak azok számára hozzáférhető, akik tudnak a létezéséről.
Szerzői jog bizonyítása, követés, újlenyomatolás.

KRIPTOGRÁFIA - ÁTTEKINTÉS 1

TÖRTÉNELEM:

- Csak **katonai, diplomáciai**, politikai alkalmazások;
- **Civil** alkalmazások is, 1977 után (számítástechnika elterjedése).

TECHNIKA:

- **Szimmetrikus vagy titkos kulcsú rejtjelezés**
  kulcscsere biztonságos csatornán;
- **Aszimmetrikus vagy nyilvános kulcsú rejtjelezés**
  nincs szükség biztonságos csatornára;
  1976 óta, (adatátvitel elterjedése, nyilvános csatornák)

KRIPTOGRÁFIA - ÁTTEKINTÉS 2 MATEMATIKA

Egyirányú függvények:

könnyű kiszámítani, de nehéz invertálni.

- **Prímtényezős felbontás**
- **Diszkrét logaritmus**
- **Diszkrét gyökvonás**

Egyirányú csapóajtó függvények:

könnyű kiszámítani, de egy (titkos) kulcs hiányában nehéz invertálni, viszont annak birtokában ez is könnyű feladat.

Algoritmusok:

- **Behelyettesítés**
- **Keverés**

Véges, diszkrét halmazok algebrái:

- **Prím méretű mezők: GF(p):**
  - modulo egész aritmetika
- **Prímhatvány méretű mezők:GF(p^m):**
  - modulo polinom algebra
  - elliptikus görbe algebra
- **Telezsák algebra.**

THE SCIENCE of CRYPTOGRAPHY

Cryptography is nothing more than a mathematical framework for discussing the implications of various paranoid delusions.

Don Alvarez

Peter Gutmann: Cryptography and Data Security, University of Auckland, New Zealand, Course Handout

TÖRTÉNELEM

Az ADATVÉDELEM, az ADATBIZTONSÁG és a KRIPTOLÓGIA TÖRTÉNELME

The HISTORY of DATA SECURITY, DATA PROTECTION and CRYPTOLOGY

Die GESCHICHTE von DATENSCHUTZ, DATEN SICHERHEIT und von KRYPTOLOGIE

REJTJELZÉS AZ ÓKORBAN
SZTEGÁNOGRÁFIA

- **ASSZUR BANIPAL** (i.e.669-i.e.627):
  - rabszolga kopaszra nyírt fejbőrére írt, és
  - a kinőtt hajjal tikosította.
- **DÉMERATUSZ** (i.e.519-i.e.465)
  - értesítette **Spártát Xerxes** görögök elleni inváziójáról.
  - fából készült irótáblára kapcolta fel a támadási tervet, majd ezt lefedte viasszal, hogy üresnek látszódjon.
  - forrás: **POLÜBIOSZ (POLYBE,** Megalopolis: i.e. 200-i.e.120):

REJTJELZÉS AZ ÓKORBAN
KEVERŐ REJTJELEZÉS

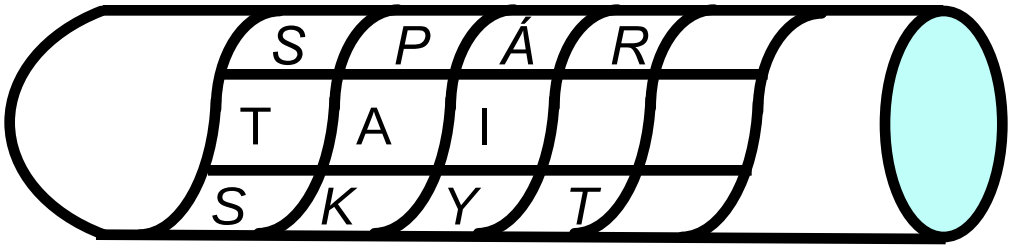
- **LÜZANDROSZ spártai hadvezér** (kb. i.e. 400)
  - a perzsa határ mentén várta a parancsot kormányától, amelyet egy rabszolga hozott meg puha övére írt összekevert betűk formájában (**keverés, transzpozició**).
  - Lüzandrosz parancsnoki pálcája végén levő üregbe helyezte, majd csavarvonalban feltekerte arra.
  - A henger alkotói mentén olvasható lett a szöveg.
  - Ennek megfelelően hazatért Spártába, ami lehetővé tette a görögöknek, hogy **Nagy Sándor** (i.e.356, 336 - i.e. 323) alatt hatalomra jussanak Keleten
  - forrás: **PLUTÁRKHOSZ** (i.e.50-125) görög történetíró.

A PHAISTOS-i KORONG

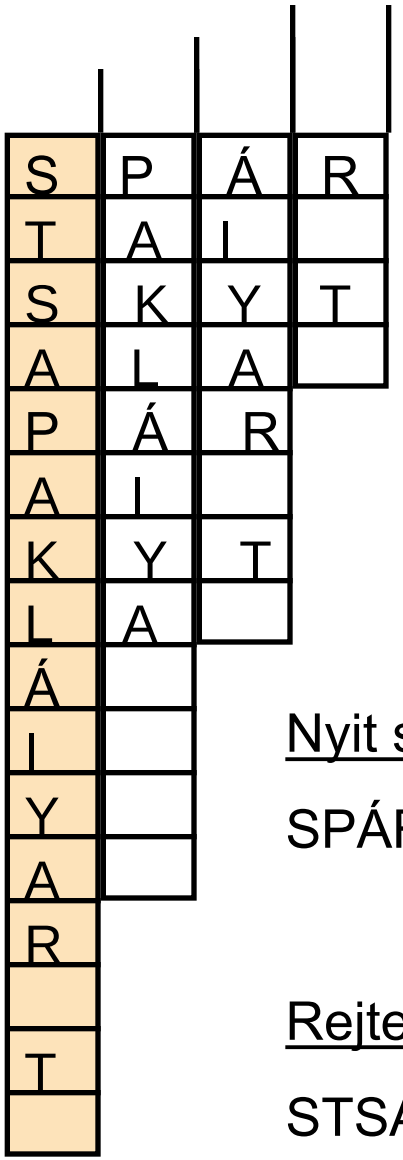
16 cm átmérőjű krétai-minoita rejtjelzett korong

Kre. 17. század.

Nach: F. L. Bauer: Entzifferte Geheimnisse



Adott átmérőjű henger alakú rúdra feltekert pergament szalag.



A SPÁRTAI SKYTALA: KEVERŐ (TRANSZPOZÍCIÓS) REJTJELEZÉS

Nyit szöveg:

SPÁRTAI SKYTALA

Rejtett szöveg:

STSAPAKLÁIYAR T

Ovid (Publius Ovidius Naso) 43 v. Chr. bis 18 n. Chr

ARS AMATORIA)

Conscia cum possit scriptas portare tabellas,
Quas tegat in tepido fascia lata sinu?
Cum possit sura chartas celare ligatas,
Et vincto blandas sub pede ferre notas?
Caverit haec custos, pro Charta conscia tergum
Praebeat inque suo corpore verba ferat.
Tuta quoque est fallitque oculos e lacte recenti
Litera: carbonis pulvere tange; leges.
Fallet et humiduli quae fiet acumine lini
Et feret occultas pura tabella notas.
Affuit Acrisio servandae cura puellae;
Hunc tamen illa suo crimine fecit avum.

(Verses 621-632)

OVID: THE ART OF LOVE (staganography)

Book III Part XV: Play Cloak and Dagger

English by A. S. Kline 2001;

When a knowing maid can carry letters you've penned,
concealed in the deep curves of her warm breasts?
When she can hide papers fastened to her calf,
or bear charming notes tied beneath her feet?
The guard's on the look-out for that, your go-between
offers her back as paper, and takes your words on her flesh.
Also a letter's safe, and deceives the eye, written with fresh milk;
you read it by scattering it with crushed ashes.
And those traced out with a point wetted with linseed oil,
so that the empty tablet carries secret messages.

OVID: LIEBENSKUNST

PUBLII OVIDII NASONIS

ARTIS AMATORIAE

LIBRI TRES.

Ovids Liebeskunst

Berichtigt, überſetzt und erklärt

von

Heinrich Lindemann.

Leipzig.

Verlag von Wilhelm Engelmann.

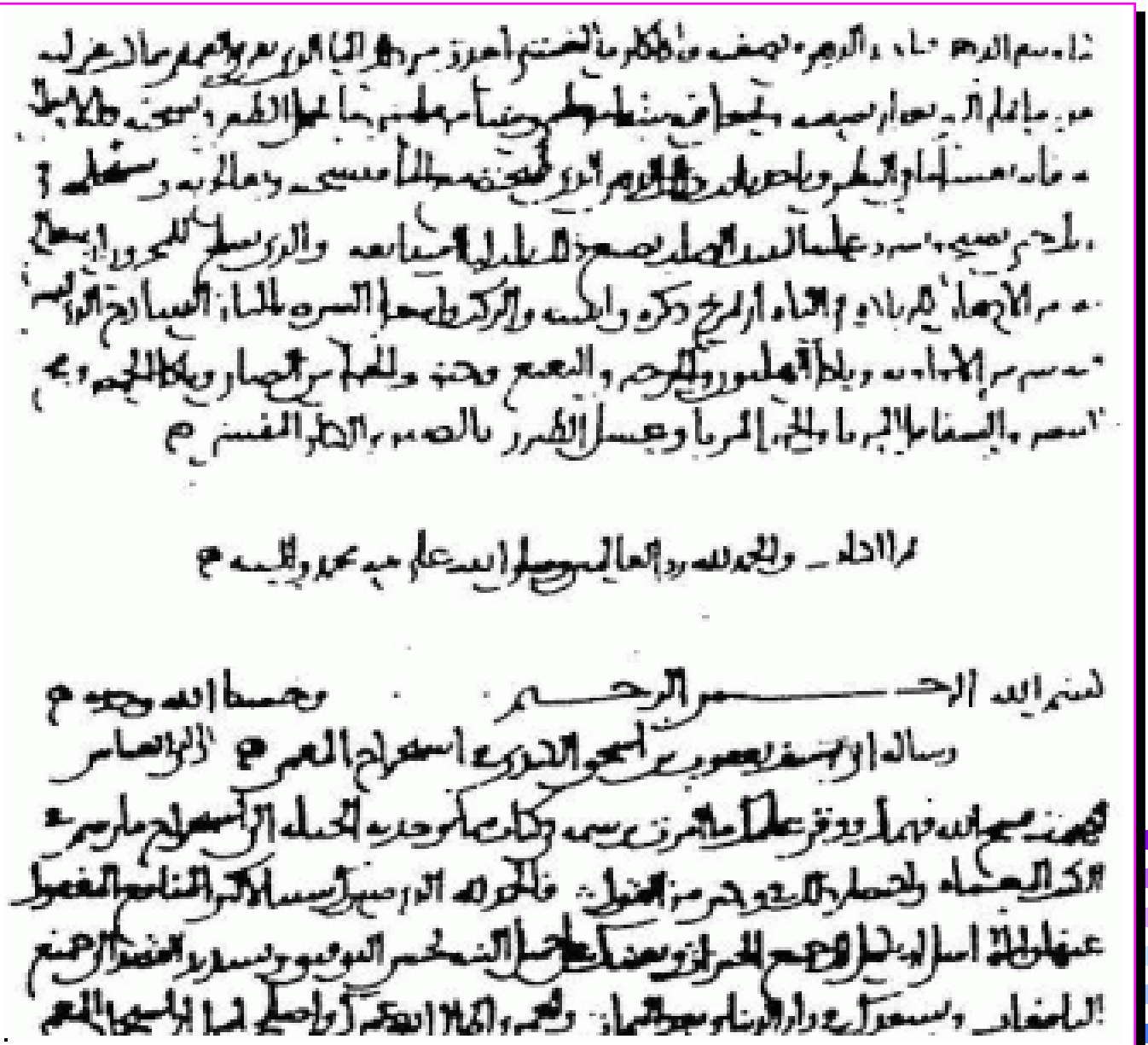
1861.

Die an der warmen Brust unter der Binde ihn birgt?
Da sie doch kann das Papier, an der Wade befestigt, verbergen,
Unter gebundenem Fuß tragen die Worte der Gunst?
Sähe der Hüter das vor, so reich' als Papier die Vertraute
Dar den Rücken; die Schrift trage ihr eigener Leib.
Sicher auch sind und entgehen dem Blick Buchstaben mit frischer
Milch; thu Kohlenstaub drüber, so liest du sie leicht.
Auch ein Briefchen, gemacht mit der Spitze des saftigen Leines,
Täuschet und bringt, ganz rein, eine verborgene Schrift.

Al-Kindi

Arab pharmacologist, musician, writer, philosopher, astronomer and calligrapher

First page of Al-Kindi's 9th century *Manuscript on Deciphering Cryptographic Messages*



Kama Sutra : Mlecchita-Vikalpa

- **Mlecchita-Vicalpa**
  - it is an ancient form of encryption prescribed by the Kama Sutra
  - Number 45 on the list of „arts a woman should learn”.
- There are two types of this art,
- The first is **kautiliam**,
  - letter substitutions are determined by phonetic relationships (consonants become vowels, etc.).
- The second is **muladeviya**
  - a reciprocal alphabet with a=b arbitrary exchanges of one letter for another (Cesar encryption with one step).

- Signs
- ँ ं ः
- Independent vowels
- ऄ अ आ इ ई उ ऊ ऋ ऍ ऎ * ए ऐ ऑ ऒ * ओ औ
- Consonants
- क ख ग घ ङ च छ ज झ ञ ट ठ ड ढ ण त थ द ध न ऩ प फ ब भ म य र ऱ ल ळ ऴ व श ष ह
- Various signs
- ़ ऽ
- Dependent vowel signs
- ा ि ी ु ू ृ ॄ ॅ ॆ े ै ॉ ॊ ो ौ
- Various signs
- ् ॐ ॑ ॒ ॓ ॔
- Additional consonants
- क़ ख़ ग़ ज़ ड़ ढ़ फ़ य़
- Generic additions
- ॠ ॡ ॢ ॣ । ॥
- Digits
- ० १ २ ३ ४ ५ ६ ७ ८ ९
- Devanagari-specific additions
- ॰

ROVÁSÍRÁS

Hun-Magyar-Székely Rovásírás

İ I H GY G F É E D CS C B Á A

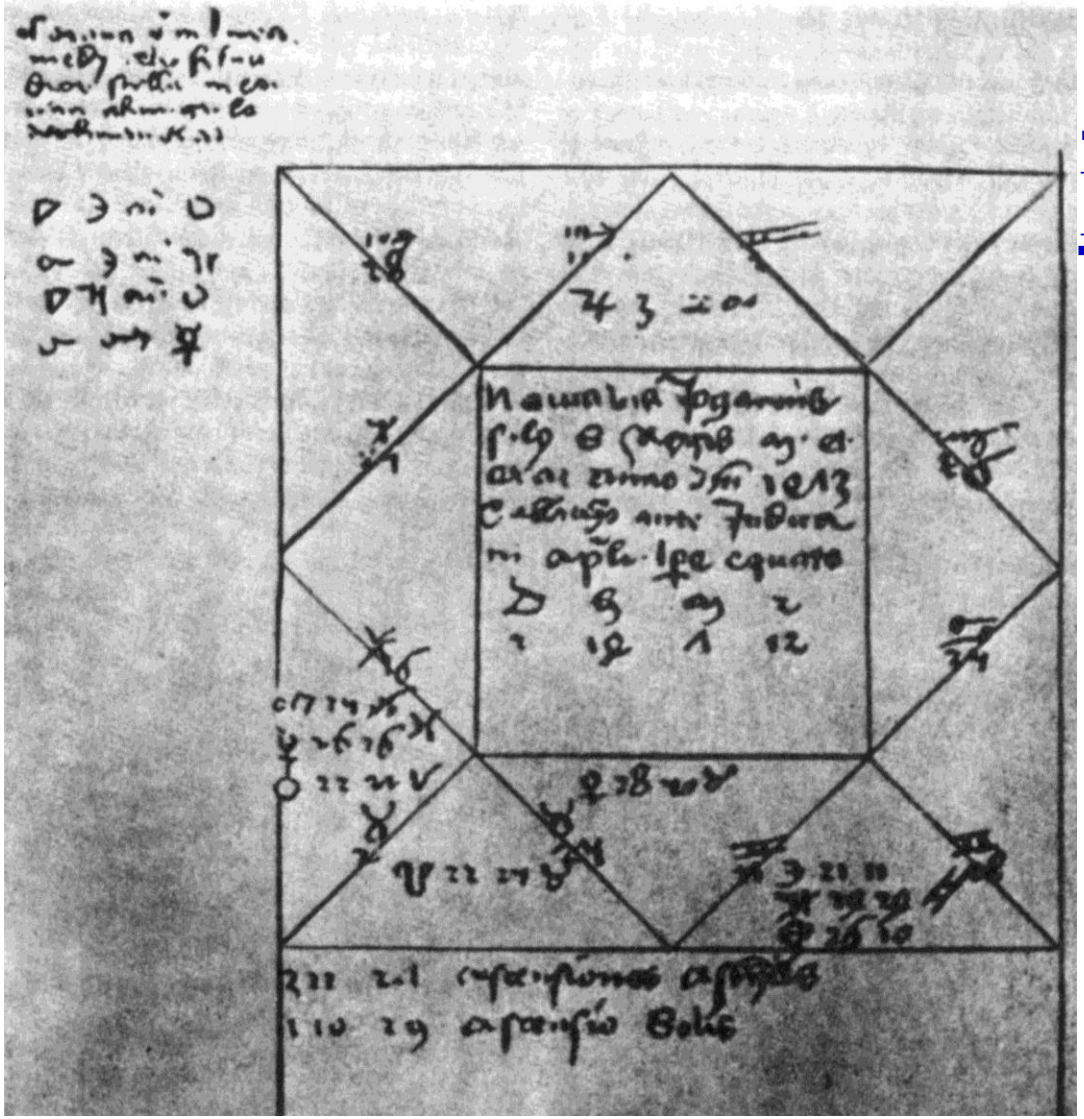
S R P Ö Ö Ó O NY N M LY L EK AK J

ZS Z V Ü Ü Ú U TY T SZ AS

1000 100 50 10 5 1

REJTJELZÉS A KÖZÉPKORBAN

- a Római Birodalom hanyatlása után a rejtjelezés is közel **1000 évig stagnált**.
- a matematika fellegvára az **arab világ** volt:
  - **ALGORITMUS**:
    Mukhammed ibn Musa Al Khwarizmi (Khoresmi) (IX.sz.) nevű arab matematikustól származik.
- **XII-XIII. században** indult fejlődésnek:
  - **kódbehelyettesítések**:
    - rövidítések,
    - rejtet v. ismeretlen jelek, szóképek;
  - **többábécés** (polialfabetikus) **behelyettesítések**;



CORVIN JÁNOS HOROSZKÓPJA 1473

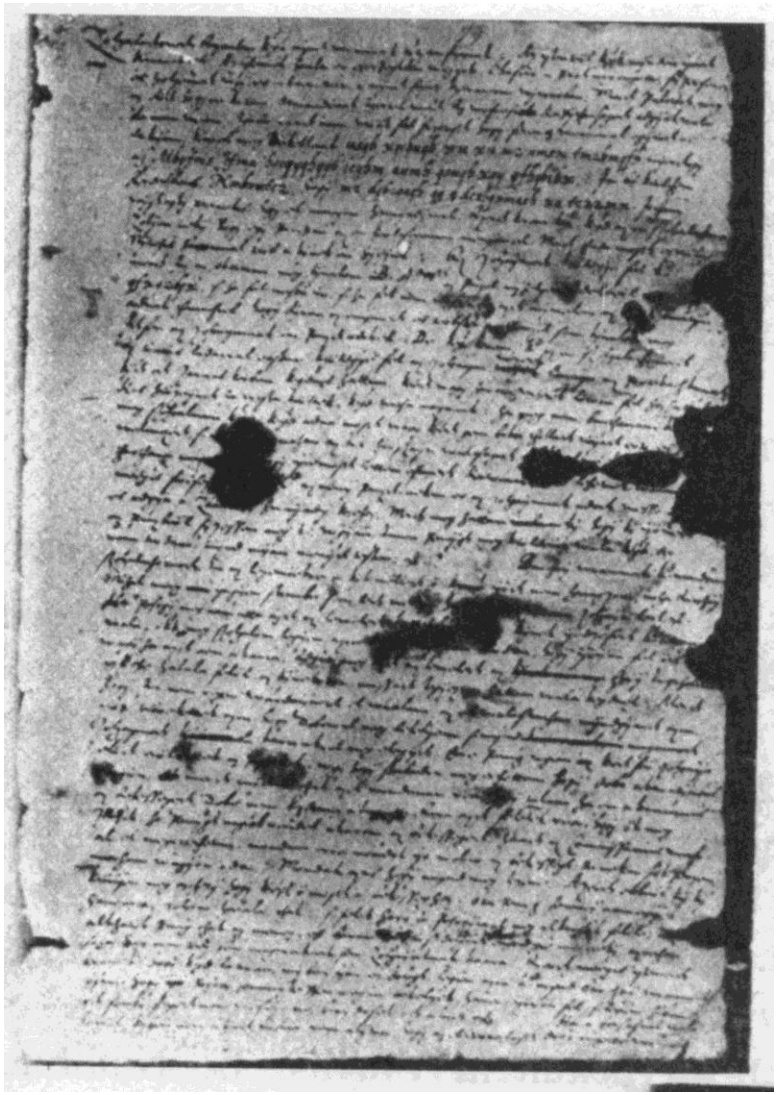
Az ELSŐ MAGYARORSZÁGI TITKOSÍRÁSÚ DOKUMENTUM

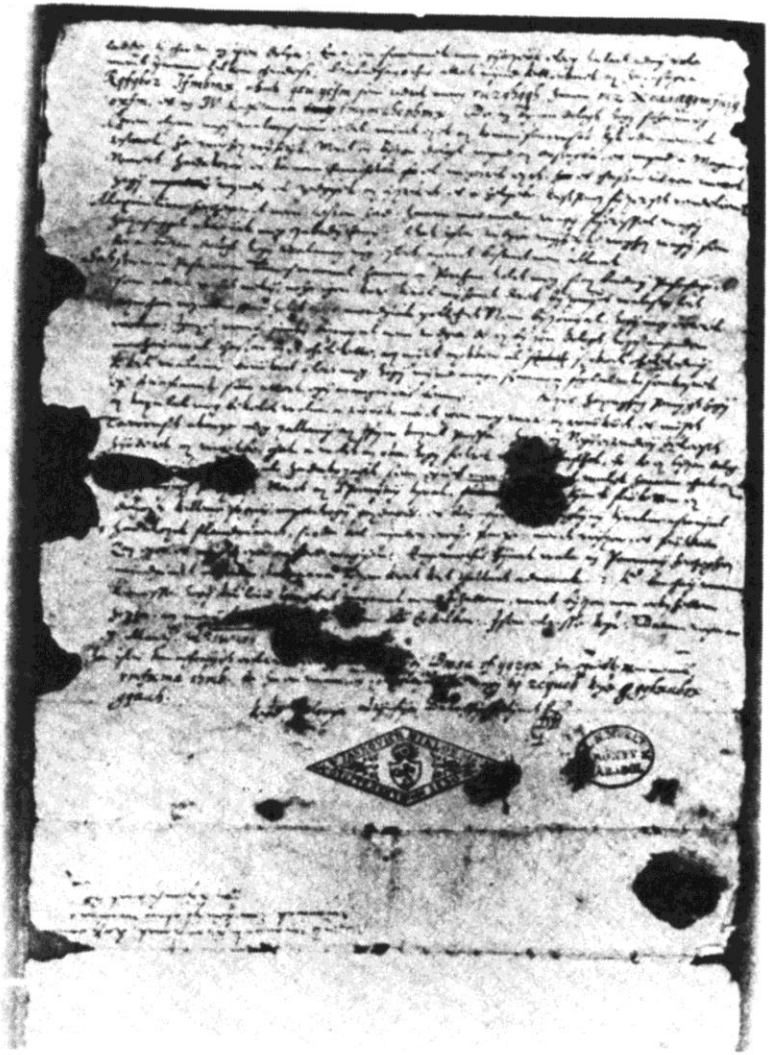
Révay Zoltán: Titkosírások; p.70.

REJTJELEZŐ KERÉK - CIPHER WHEEL: XVIII század

- Feltételezhető, hogy a fennmaradt legrégebbi ilyen rejtjelező szerkezet.
- Francia nyelvre készült.
- West Virginiából vásárolta az NSA.
- Hasonló szerkezetet irt le: Jefferson (1743-1826) és François Bacon, 1605.

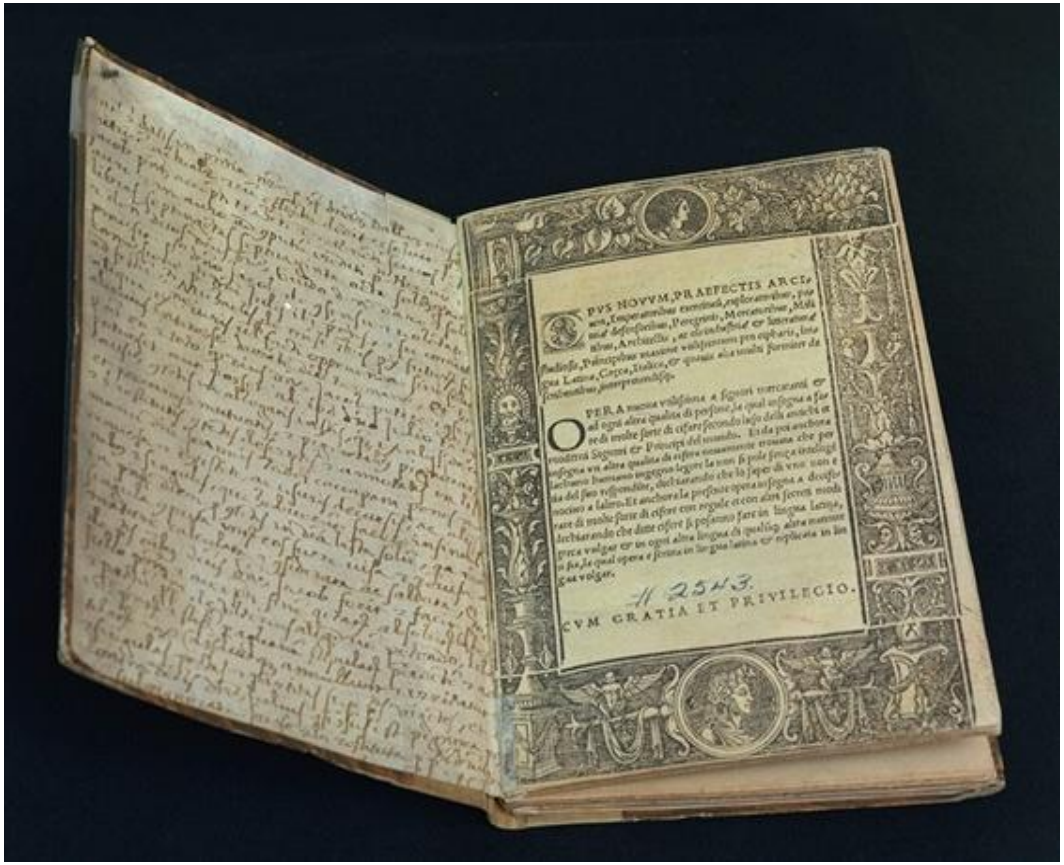
BALASSI BÁLINT RÉSZLEGES REJTJELZÉSŰ LEVELE - 1588. március 7.





Révay Zoltán: Titkosírások; p.81.

RITKA KRIPTOLÓGIAI KÖNYVEK 1.



AZ ELSŐ VALAHA PUBLIKÁLT KRIPTOLÓGIAI KÖNYV MÁSODIK KIADÁSA

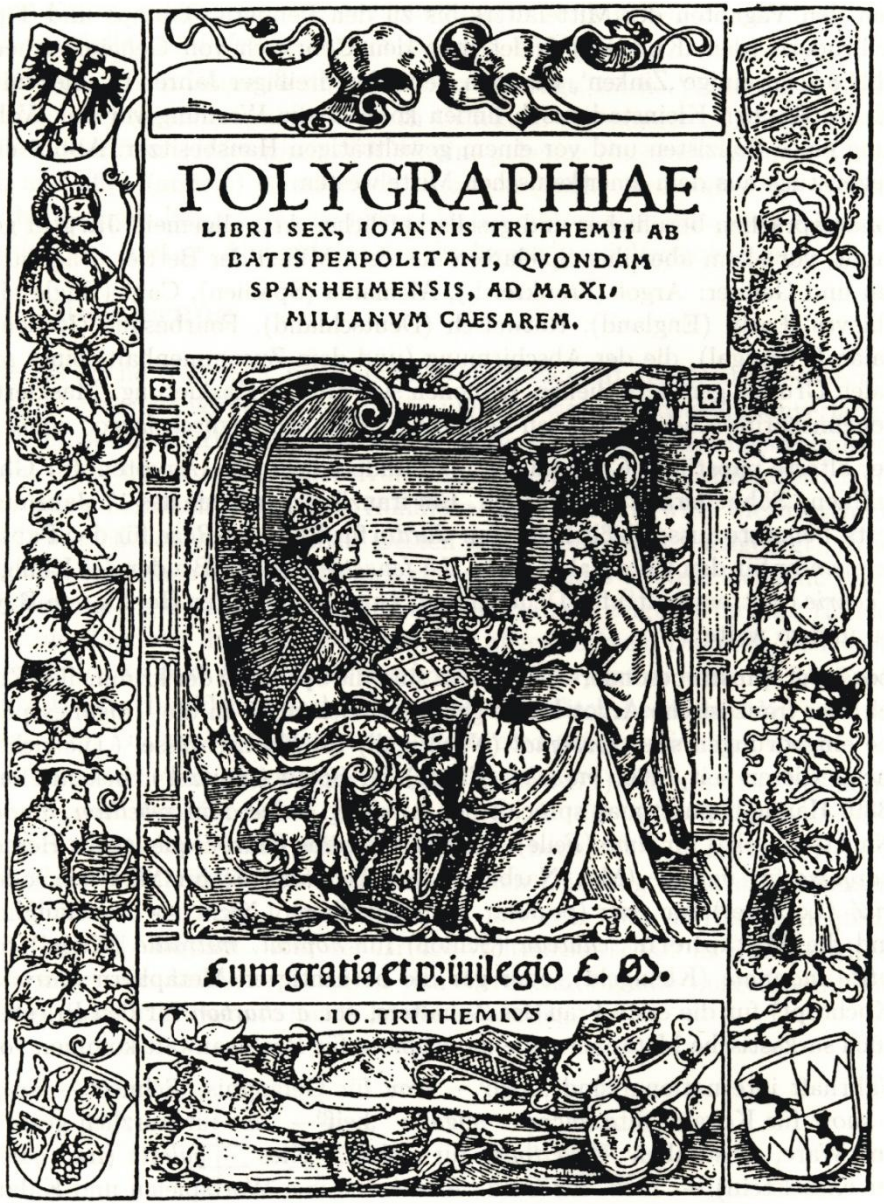
The National Cryptologic Museum, NSA, USA

TRITHEMIUS: POLIGRAPHIAE

Titelseite (Holzschnitt) des ersten gedruckten Werkes über Kryptographie.

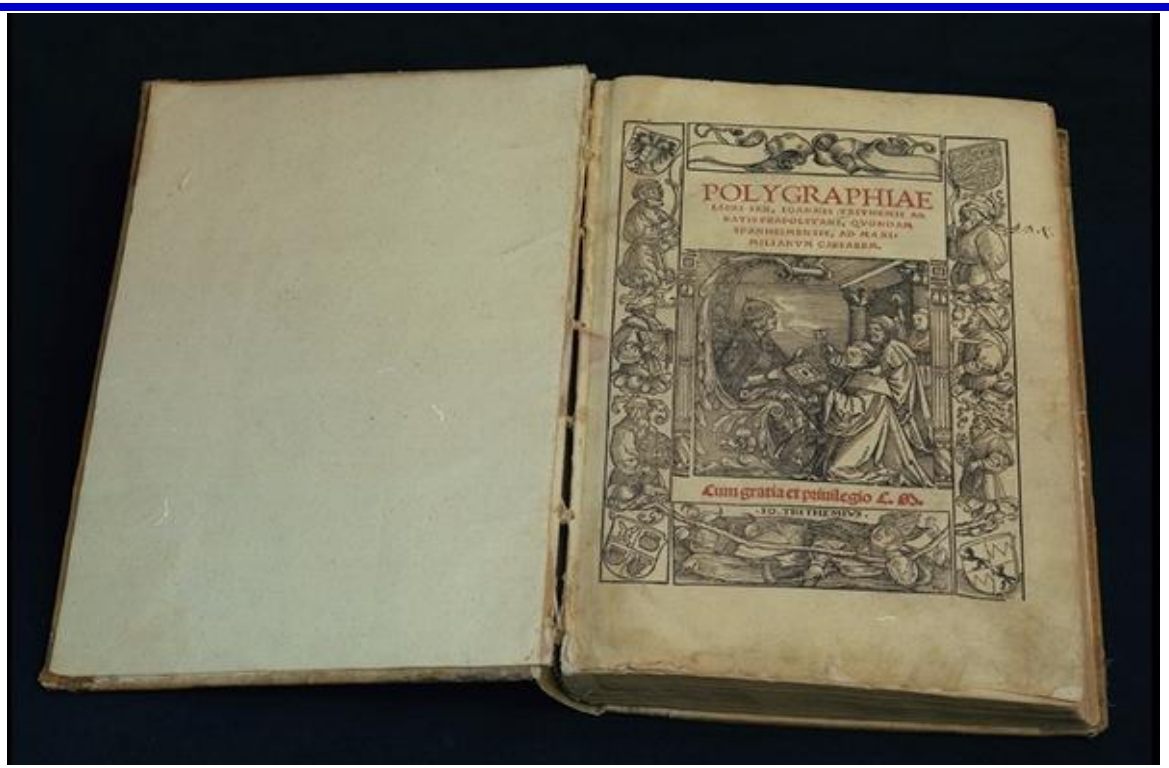
geschrieben: 1508

gedruckt: 1518



Nach: F. L. Bauer: Entzifferte Geheimnisse

RITKA KRIPTOLÓGIAI KÖNYVEK 2.



Johannes Trithemius 1462-1516

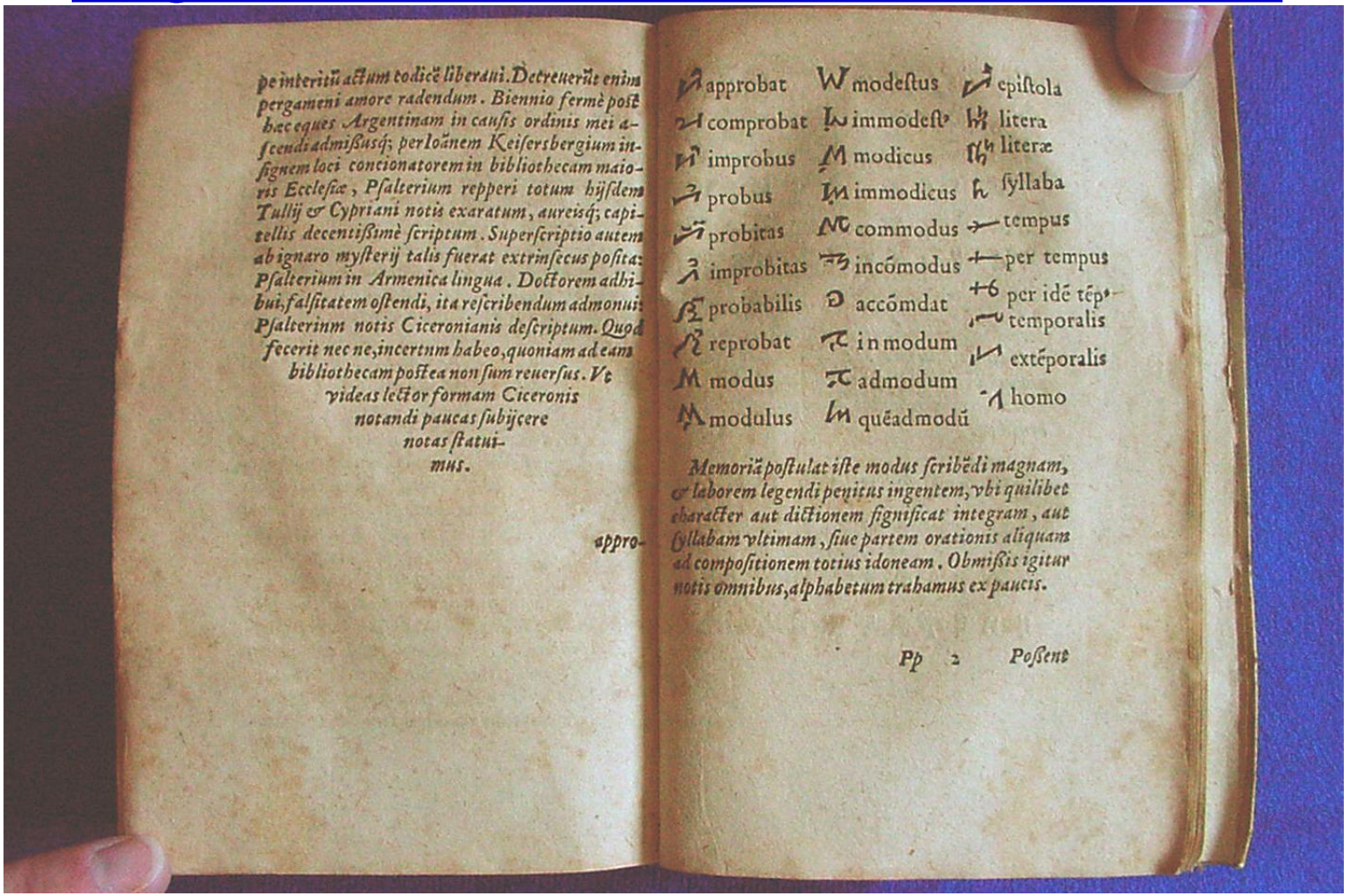
A NYUGATI VILÁG MÁSODIK KRIPTOLÓGIAI KÖNYVE
ELSŐ KIADÁS
„ P O L I G R A P H I A E „

The National Cryptologic Museum, NSA, USA

JOHANNES TRITHEMIUS.

Polygraphiae libri sex...Accessit clavis polygraphiae liber unus, eodem authore

Cologne: Ioannes Birckmannus & Theodorus Baumius, 1571



pe interitū actum eodicē liberaui. Decreuerūt enim pergameni amore radendum. Biennio fermè post hæc eques Argentinam in causis ordinis mei ascendi admißusq; per loānem Keisersbergium insignem loci concionatorem in bibliothecam maioris Ecclesiæ, Psalterium repperi totum hijsdem Tullij & Cypriani notis exaratum, aureisq; capitellis decentißimè scriptum. Superscriptio autem ab ignaro mysterij talis fuerat extrinsecus posita: Psalterium in Armenica lingua. Doctorem adhibui, falsitatem ostendi, ita rescribendum admonui: Psalterinm notis Ciceronianis descriptum. Quod fecerit nec ne, incertum habeo, quoniam ad eam bibliothecam postea non sum reuersus. Vt videas lector formam Ciceronis notandi paucas subijcere notas statuimus.

appro-

approbat
comprobat
improbus
probus
probitas
improbitas
probabilis
reprobat
modus
modulus

modestus
immodest⁹
modicus
immodicus
commodus
incōmodus
accōmdat
in modum
admodum
quēadmodū

epistola
litera
literæ
syllaba
tempus
per tempus
per idē tēp⁹
temporalis
extēporalis
homo

Memoriā postulat iste modus scribēdi magnam, & laborem legendi penitus ingentem, vbi quilibet character aut dictionem significat integram, aut syllabam vltimam, siue partem orationis aliquam ad compositionem totius idoneam. Obmissis igitur notis omnibus, alphabetum trahamus ex paucis.

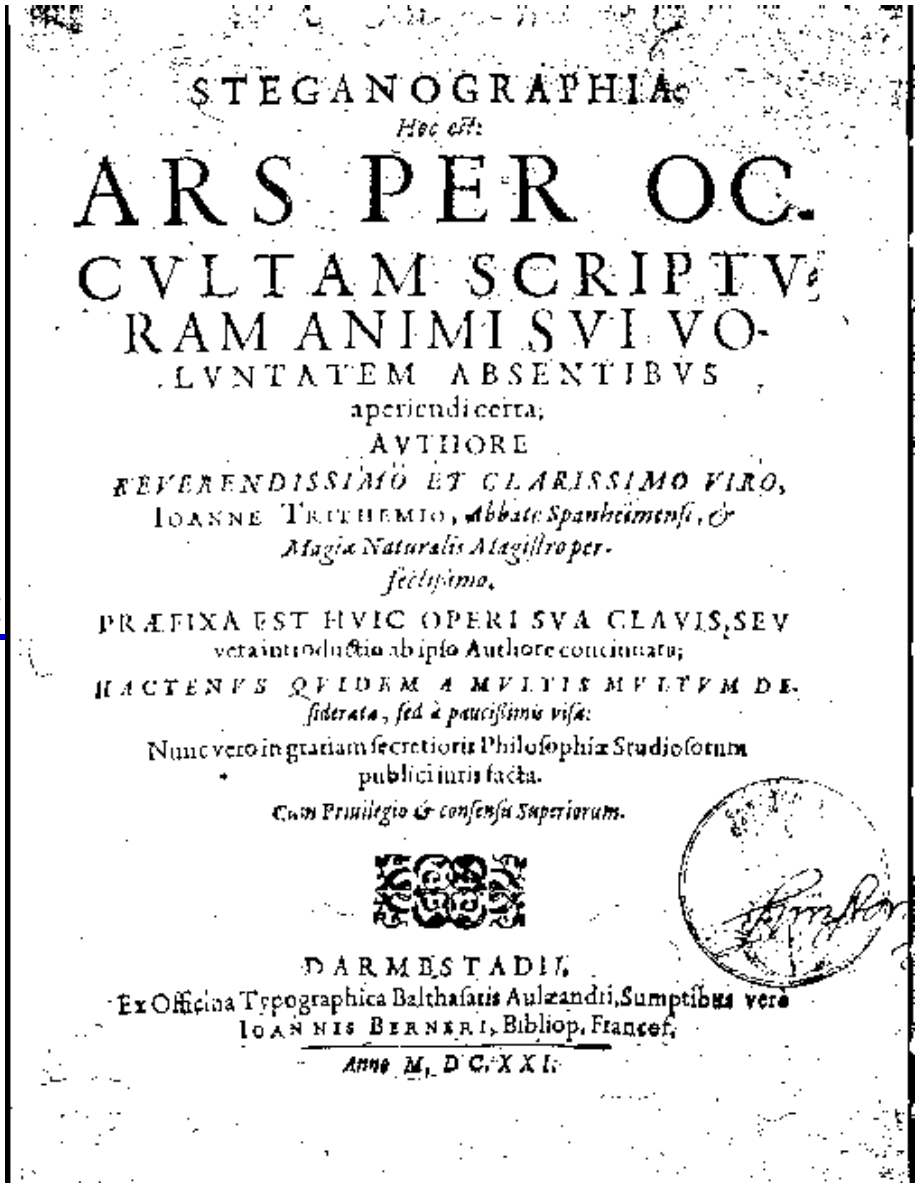
Pp 2 Posſent

1462-1516
Johannes Trithemius

STEGANOGRAPHIA:

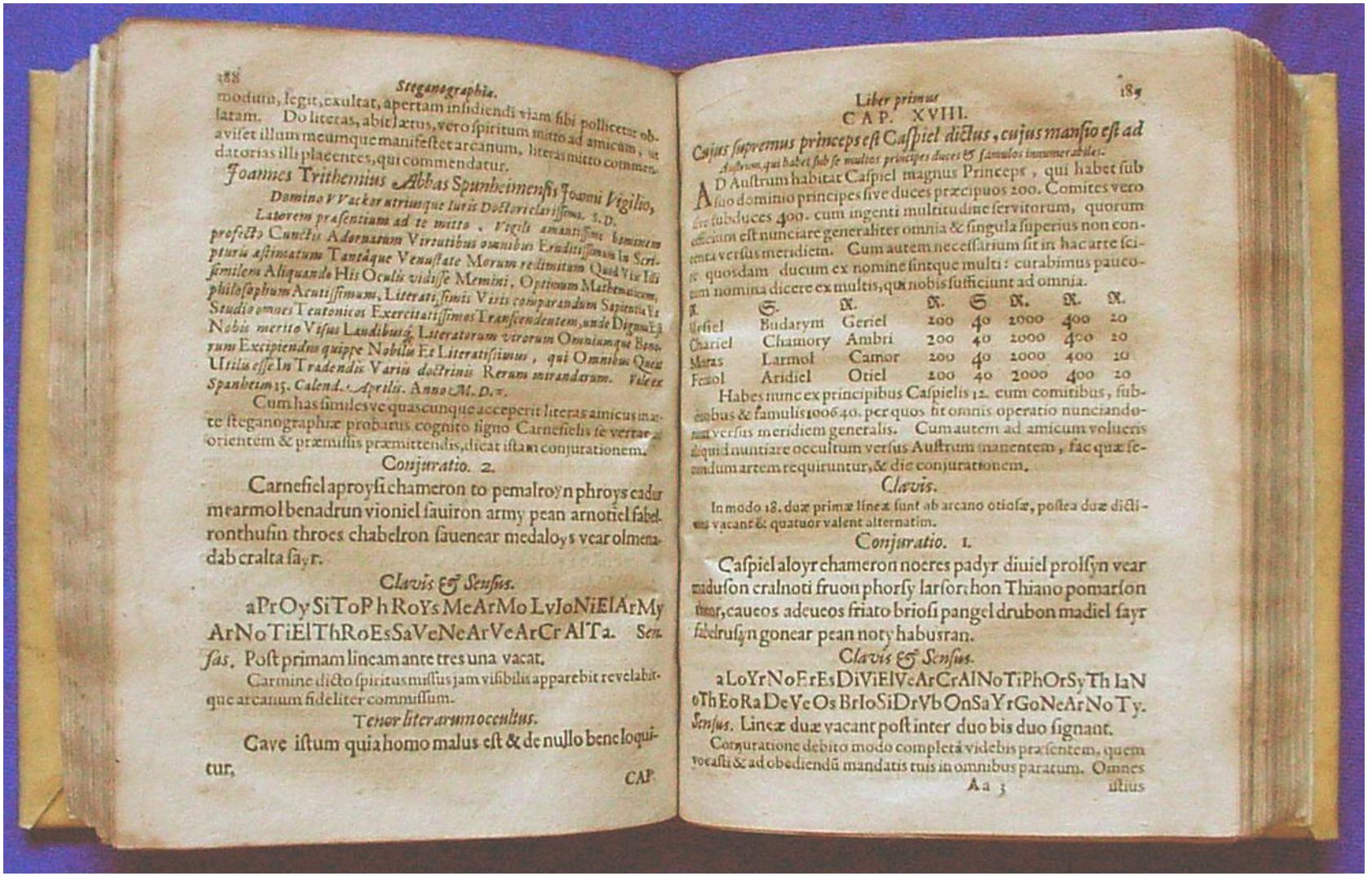
Hoc est: ARS PER OCCVLTAM SCRIPTVRAM ANIMI SVI VOLVNTATEM ABSENTIBVS aperiendi certa; AVTHORE *REVERENDISSIMO ET CLARISSIMO VIRO,*

IOANNE TRITHEMIO,



STEGANOGRAPHIAE
Hoc eſt:
ARS PER OC.
CVLTAM SCRIPTV
RAM ANIMI SVI VO-
LVNTATEM ABSENTIBVS
aperiendi certa;
AVTHORE
REVERENDISSIMO ET CLARISSIMO VIRO,
IOANNE TRITHEMIO, Abbate Spanheimenſi, &
Magiæ Naturalis Magiſtro per-
fectiſſimo.
PRÆFIXA EST HVIC OPERI SVA CLAVIS, SEV
vera intra ductio ab ipſo Authore concinnata;
HACTENVS QVIDEM A MVLTIS MVLTVM DE-
ſiderata, ſed à paucisſimis viſa:
Nunc vero in gratiam ſecretioris Philoſophiæ Studioſorum
publici iuris facta.
Cum Priuilegio & conſenſu Superiorum.
DARMESTADII,
Ex Officina Typographica Balthaſaris Aulæandri, Sumptibus vero
IOANNIS BERNERI, Bibliop. Francef.
Anno M. DC. XXI.

Johannes Trithemius: *Steganographia:* Mainz: Christophorus Küchlerus, 1676.



188 *Steganographia.*

modum, legit, exultat, apertam insidiendi viam sibi pollicetur: obsecratum. Do literas, abit: lætus, vero spiritum mitto ad amicum, ut aviset illum meumque manifestet arcanum, literas mitto commendatorias illi placentes, qui commendatur.

Joannes Trithemius Abbas Spunheimensis Joanni Vigilio, Domino Wackarstrunque Iuris Doctori clarissimo. S. D.

Latorem præsentium ad te mitto, Vigili amantissime hominem profectò Cunctis Adornatum Virtutibus omnibus Eruditissimum Scripturis æstimatum Tantâque Venustate Morum redimitum Quid Vix Ideo similem Aliquando His Oculis vidisse Memini, Optimum Mathematicum, philosophum Acutissimum, Literatissimis Viris comparandum Sapientia Vt Studio omnes Teutonicos Exercitatissimos Transscendentem, unde Dignus Es Nobis merito Visus Laudibus, Literatorum virorum Omniumque Bonorum Excipiendus quippe Nobilis Et Literatissimus, qui Omnibus Quæ Utilia esse In Tradendis Variis doctrinis Rerum mirandarum. Vale ex Spanheim 15. Calend. Aprilis. Anno M. D. .

Cum has similesve quascunque acceperit literas amicus in arte steganographiæ probatus cognito signo Carnefielis se vertat ad orientem & præmissis præmittendis, dicat istam conjurationem.

Conjuratio. 2.

Carnefiel aproysi chameron to pemalroyn phroys cadar mearmol benadrun vioniel fauiron army pean arnotiel fabelronthusin throes chabelron fauenear medaloys vear olmenadab cralta fayr.

Clavis & Sensus.

aPrOySiToPhRoYsMeArMoLvJoNiElArMy ArNoTiElThRoEsSaVeNeArVeArCrAlTa. *Sensus.* Post primam lineam ante tres una vacat.

Carmine dicto spiritus missus jam visibilis apparebit revelabitque arcanum fideliter commissum.

Tenor literarum occultus.

Cave istum quia homo malus est & de nullo bene loquitur,

CAP.

Liber primus 189

CAP. XVIII.

Cujus supremus princeps est Caspiel dictus, cujus mansio est ad Austrum, qui habet sub se multos principes duces & famulos innumerabiles.

AD Austrum habitat Caspiel magnus Princeps, qui habet sub suo dominio principes sive duces præcipuos 200. Comites vero sive subduces 400. cum ingenti multitudine servitorum, quorum officium est nunciare generaliter omnia & singula superius non contenta versus meridiem. Cum autem necessarium sit in hac arte scire quosdam ducum ex nomine sintque multi: curabimus pauconum nomina dicere ex multis, quæ nobis sufficiunt ad omnia.

ℵ.	S.	ℵ.	ℵ.	S	ℵ.	ℵ.	ℵ.
Ueriel	Budarym	Geriel	200	40	2000	400	20
Chariel	Chamory	Ambri	200	40	2000	400	20
Maras	Larmol	Camor	200	40	2000	400	20
Fenol	Aridiel	Otiel	200	40	2000	400	20

Habes nunc ex principibus Caspielis 12. cum comitibus, subditis & famulis 1006 40. per quos fit omnis operatio nunciando versus meridiem generalis. Cum autem ad amicum volueris aliquid nuntiare occultum versus Austrum manentem, fac quæ secundum artem requiruntur, & die conjurationem.

Clavis.

In modo 18. duæ primæ lineæ sunt ab arcano otiosæ, postea duæ dictionis vacant & quatuor valent alternatim.

Conjuratio. 1.

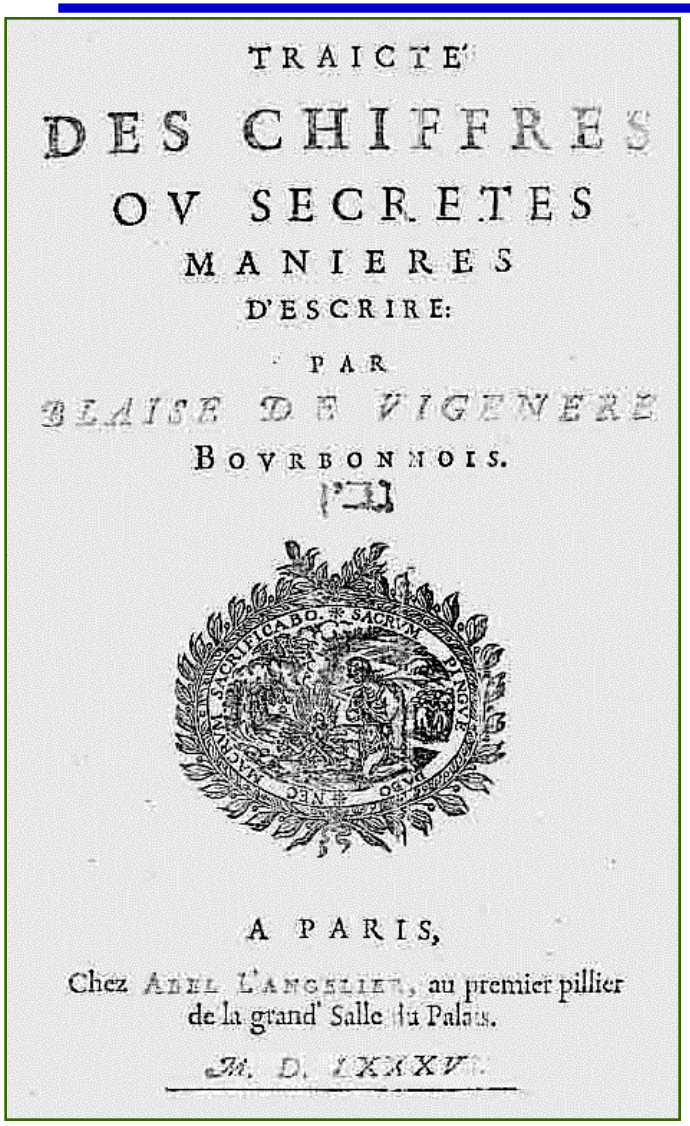
Caspiel aloyr chameron noeres padyr diuiel prolsyn vear maduson cralnoti fruon phorsy larsor: hon Thiano pomarson thar, caueos adeueos friato briosi pangel drubon madiel fayr fabedrusyn gonear pean noty habusran.

Clavis & Sensus.

aLoYrNoErEsDiViElVeArCrAlNoTiPhOrSyThIaN oThEoRaDeVeOsBrIoSiDrVbOnSaYrGoNeArNoTy. *Sensus.* Lineæ duæ vacant post inter duo bis duo signant.

Conjuratione debito modo completa videbis præsentem, quem vocasti & ad obediendū mandatis tuis in omnibus paratum. Omnes

The BOOK of BLAISE DE VIGENERE



TRAICTE'

DES CHIFFRES

OV SECRETES

MANIERES

D'ESCRIRE:

PAR

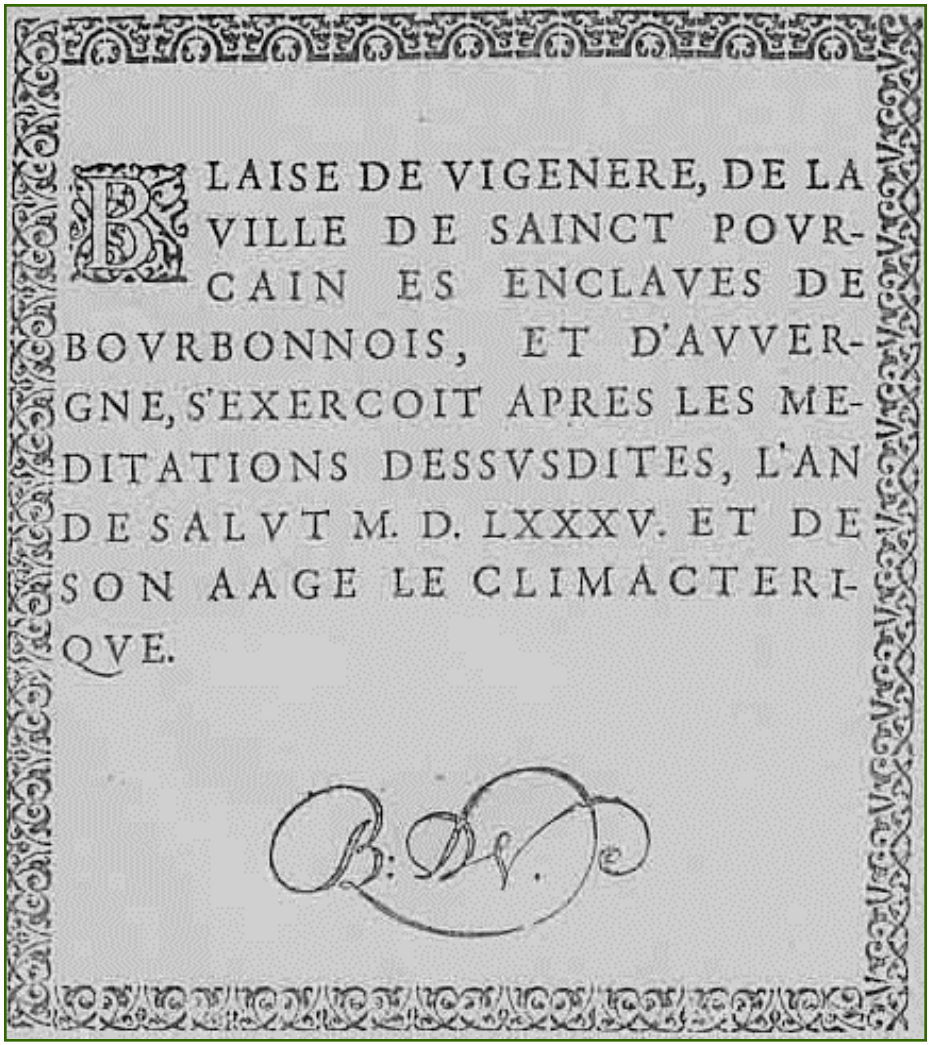
BLAISE DE VIGENERE

BOVRBONNOIS.

A PARIS,

Chez ABEL L'ANGELIER, au premier pillier de la grand' Salle du Palais.

M. D. LXXXV.



BLAISE DE VIGENERE, DE LA VILLE DE SAINCT POVRCAIN ES ENCLAVES DE BOVRBONNOIS, ET D'AVVERGNE, S'EXERCOIT APRES LES MEDITATIONS DESSVSDITES, L'AN DE SALVT M. D. LXXXV. ET DE SON AAGE LE CLIMACTERIQVE.

B: D. V.

CASANOVA and the CRYPTOGRAPHY

Five or six weeks later, she [madam d'Urfé] asked me if I had deciphered the manuscript which had the transmutation procedure. I told her that I had.

„Without the key, sir, excuse me if I believe the thing impossible."

„Do you wish me to name your key, madam?"

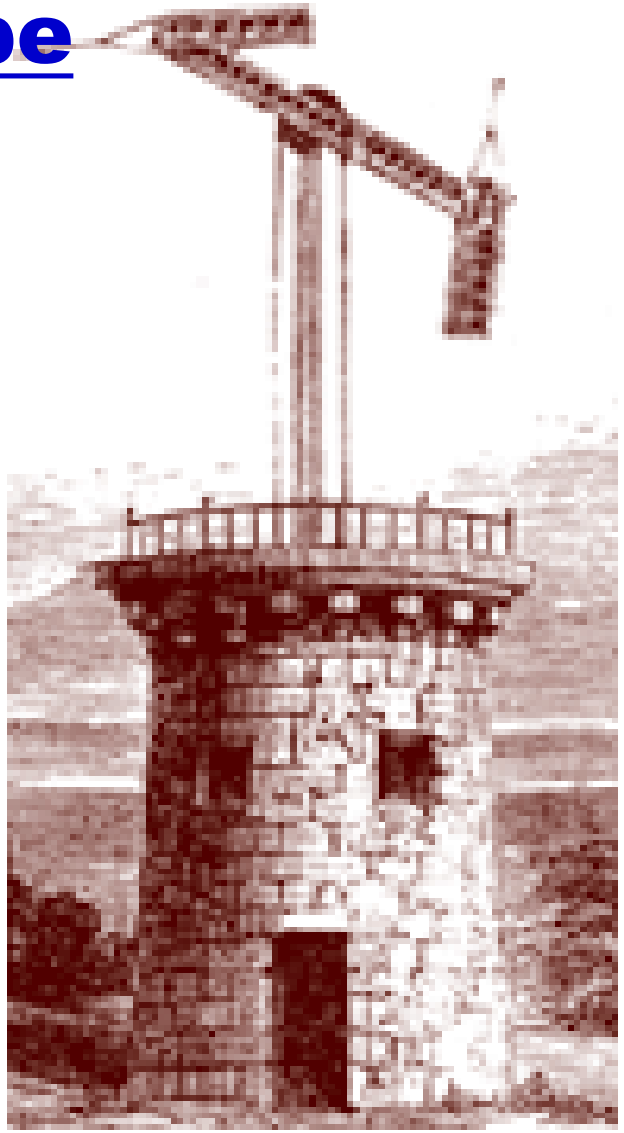
„If you please"

I then told her the key-word, which belonged to no language, and I saw her surprise. She told me that it was impossible, for she believed herself the only possessor of that word which she kept in her memory and which she had never written down.

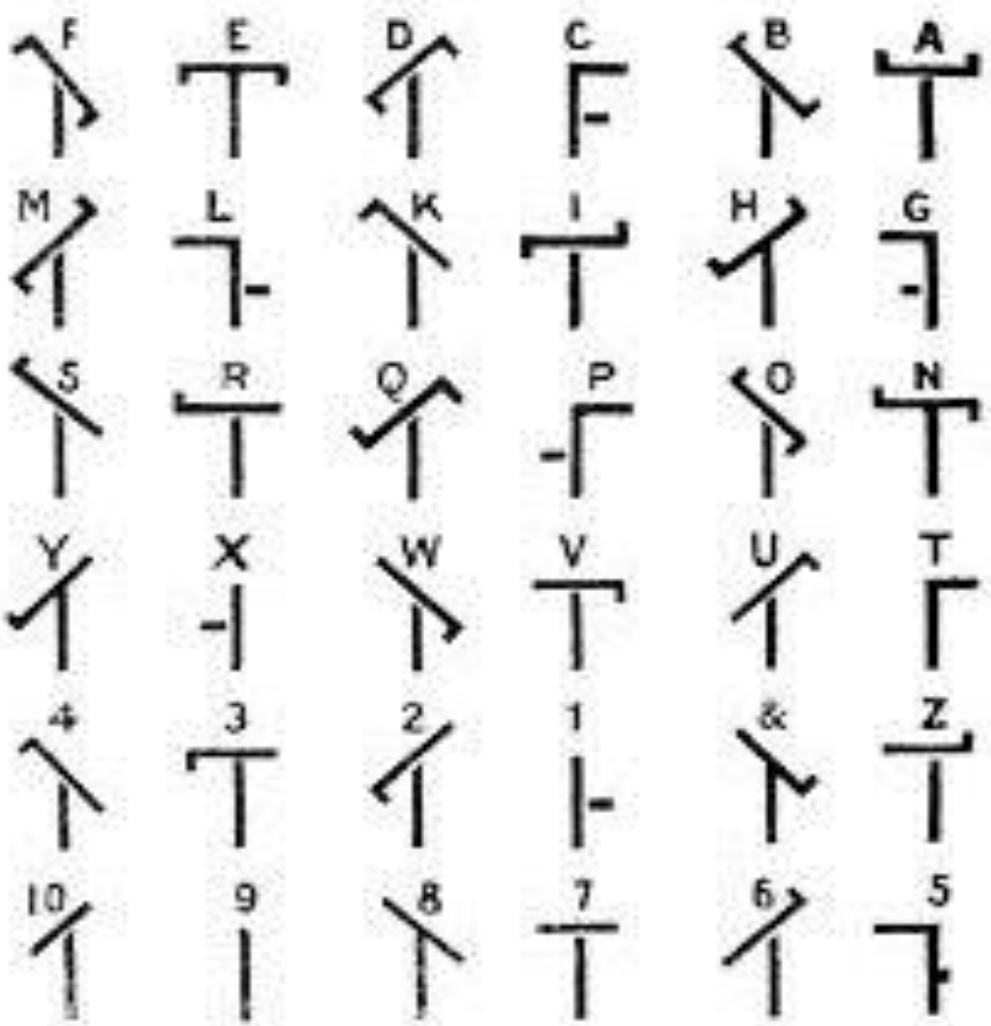
I could have told her the truth - that the same calculation which had served me for deciphering the manuscript had enabled me to learn the word - but on a caprice it struck me to tell her that a genie had revealed to me. This false disclosure fettered Madam d'Urfé to me. That day I become the master of her soul, and I abused my power. Every time I think of it, I am distressed and ashamed, and I do penance now in the obligation under which I place myself of telling the truth in writing my memoirs.

Casanova, 1757: Kahn's *The codebreakers* and Koblitz: A Course in Number Theory and Cryptography.

Secret telegraphy of Fransman Claude Chappe (1763 - 1805).



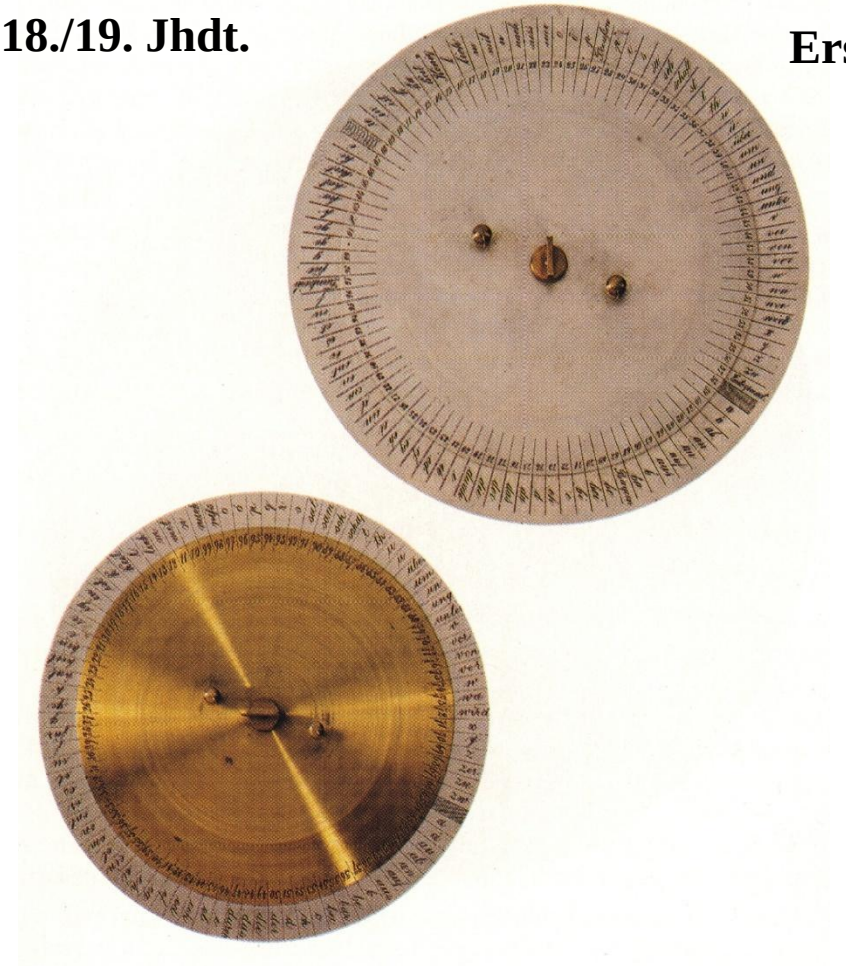
Chappe's telegraph, 1791.



- The upper part of the apparatus was made up of a movable arm and two levers to adjust its position.
- Each position indicated a letter.
- This is the used code.

CHIFFRIERGERÄTEN

Zwei Chiffrierscheiben
Vermutlich aus dem
18./19. Jhdt.

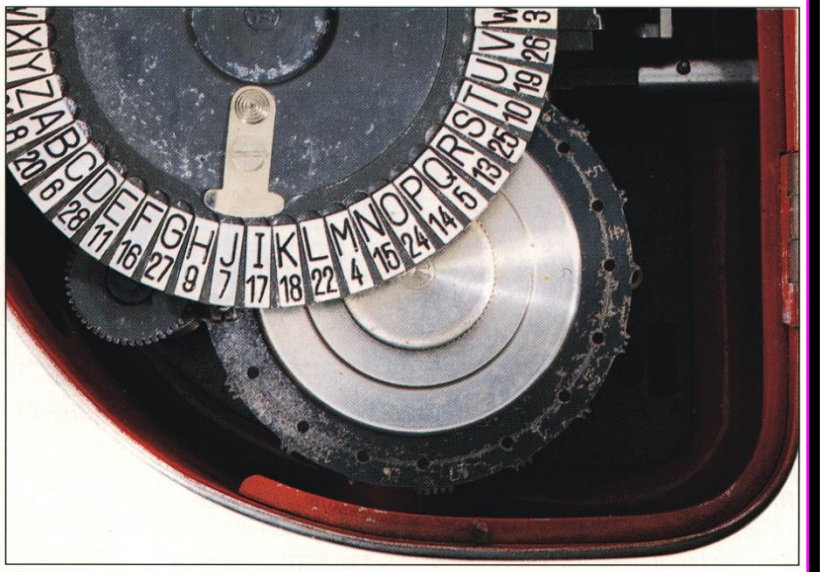


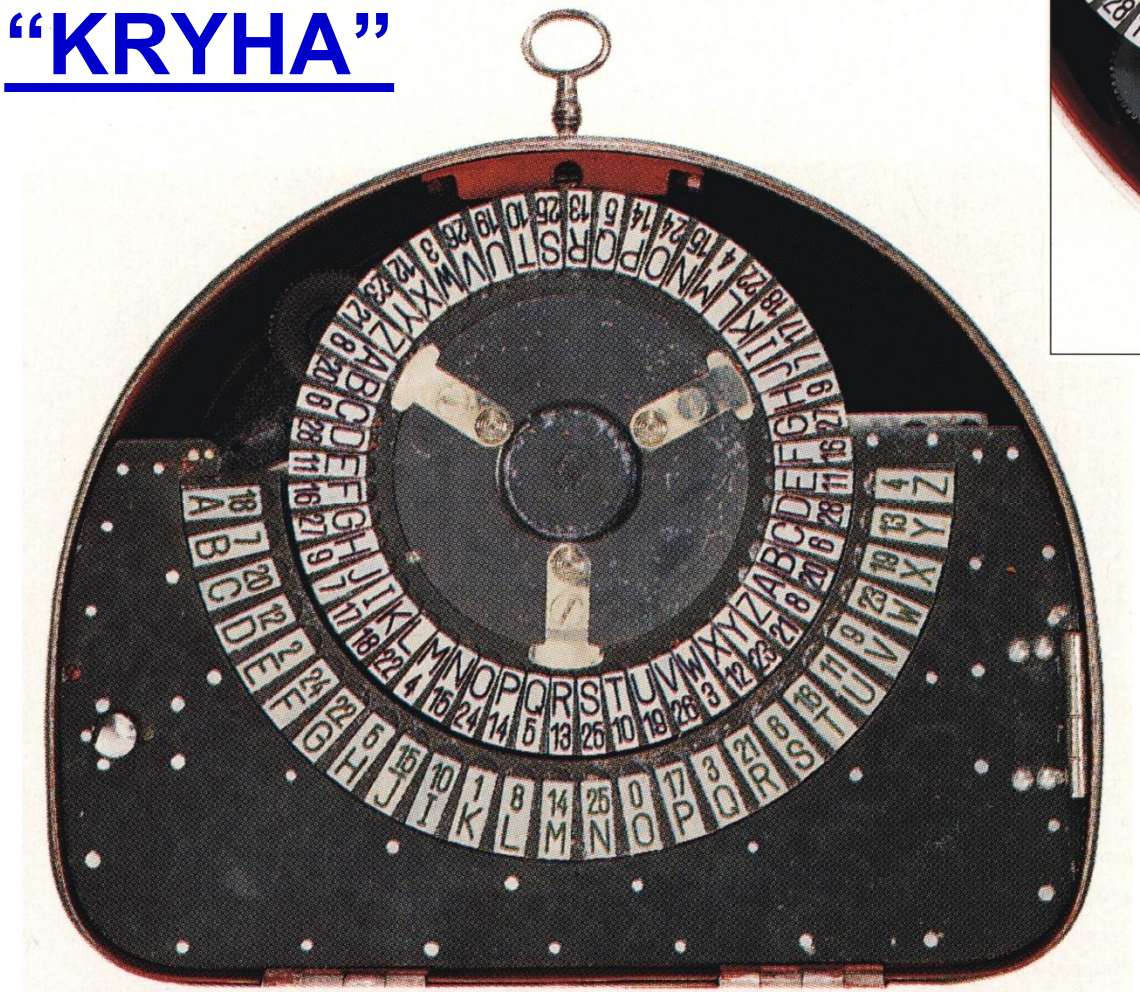
„CRYPTOGRAPH“ von Charles Wheatstone.
Polyalphabetisches Chiffriergerät in Uhrenform.

Erstmal gezeigt in Pariser Weltausstellung, 1867.

Nach:F.L.Bauer:
Entzifferte Geheimnisse

POLIALPHABETISCHE CHIFFRIERMASCHINE "KRYHA"





Alexander von Kryha,

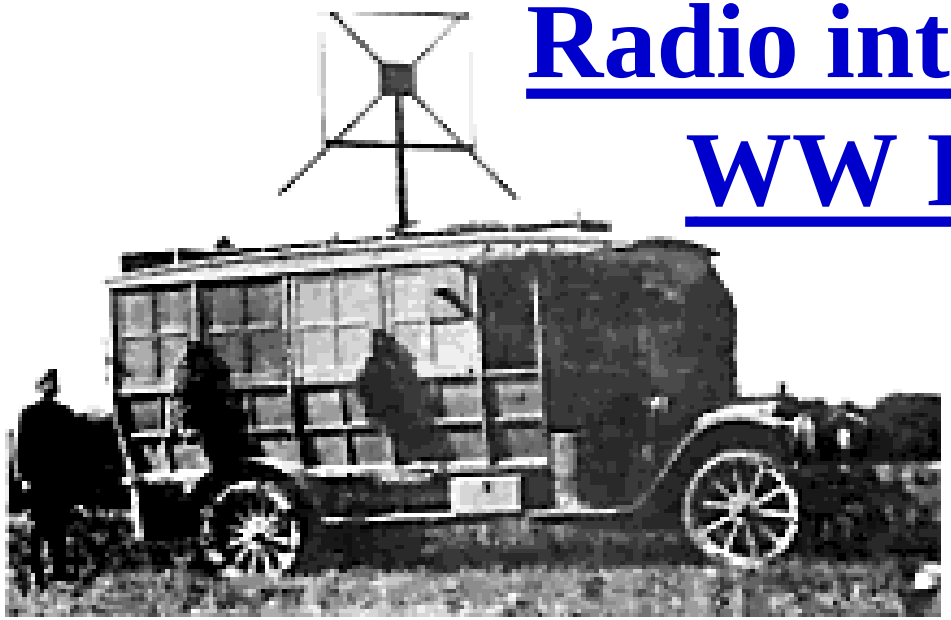
Berlin-Charlottenburg

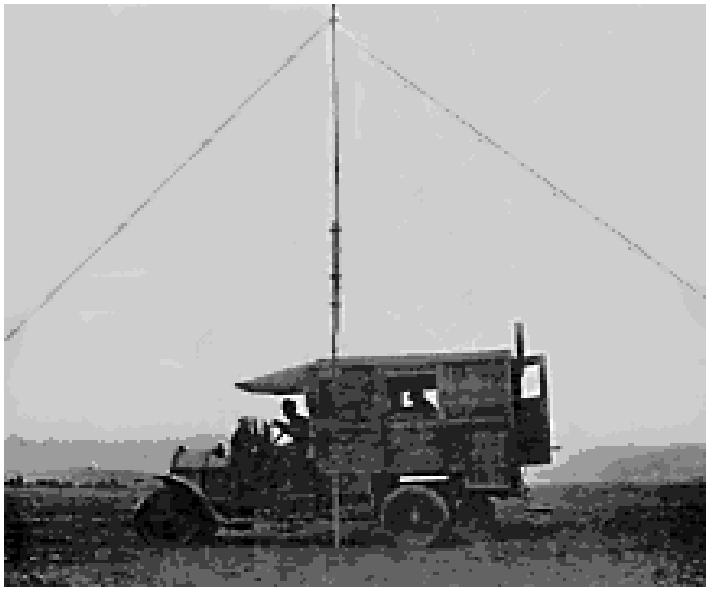
1926

Schlüssellänge: 442

Nach:F.L.Bauer:
Entzifferte Geheimnisse

Radio intelligence: WW I. + II.





József Attila: LEVEGŐT 1935. november 21.

Számon tarthatják, mit telefonoztam

s mikor, miért, kinek.

Aktákba írják, miről álmodoztam

s azt is, ki érti meg.

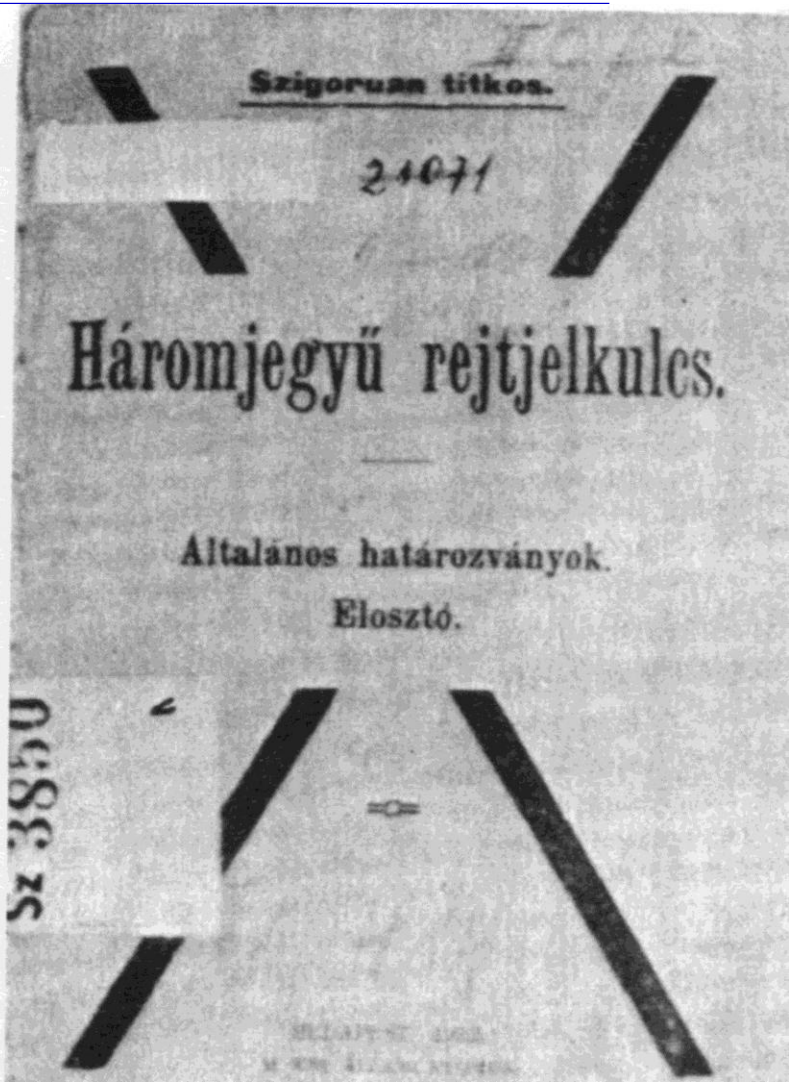
És nem sejthetem, mikor lesz elég ok

előkotorni azt a kartotékot,

mely jogom sérti meg.

HÁROMJEGYŰ REJTJELKUKCS

K. u. K. MONARCHIA HADSEREGE - 1912



HÁROMJEGYŰ REJTJELKUKCS
K. u. K. MONARCHIA HADSEREGE - 1912

Verzeichnis der Sigel.

A.

Abend (abends)	852	allgemein	488
Abteilung	214	angeordnet	110
Abschnitt	980	Anstalt	658
Abteilung	615	April	997
achter	326	Armee	999
achtzehnter	621	Arrest	380
achtundzwanzigster	409	Artillerie	243
Admiral	916	Assistenz	313
aktiv	306	Attaché	694
Alarm	334	Attentat	437
Alarmierung	785	August	977
Alarmierungstag	806	Ausnahmsverfügungen	287
Albanien	410	Automobil	662
albanesisch	675	Avise	120
Allerhöchst	770		

B.

Banus	983	Bezirkshauptmannschaft	295
Baracke	507	Bezirkswachtmeister	906
Barrikade	710	Blockhaus	729
Bataillon	139	Boot	834
Batterie	145	Bosnien	370
Befehl	346	bosnisch	998
Befestigung	666	Brigade	285
Behörde	788	Brücke	557
Bereitschaft	359	Bürgermeister	864

A jelények mutatója.

A.

adag	956	állomás parancsnok	345
agyu	639	alosztály	966
akna	905	altábornagy	482
alakulás (alakzat)	118	általános	488
albán (albánul)	675	altiszt	965
Albánia	410	április	997
alezredes	532	átirat	761
alispán	730	attaché	694
állomány	735	augusztus	977
állományfelemelés	738	Ausztria	131
állomás	538	azonnal	992

B.

bán	983	bizalmas	940
barak	507	bizalmi egyén	744
bebizonyitás	892	biztos	835
behivás	714	biztositás	964
behivójegy	739	bosnyák (bosnyákul)	998
beszállásolás	920	Bosznia	370
bíróság	818		

C.

carabiniere	743	csendőrség	231. 936
cirkáló	794	csónak	834
csapat	945	csoport	961
csapatkórház	610	cs. és kir. 613. 653. 762. 804. 854. 904	
csapattest	959	cs. k. (csász. kir.) 564. 633. 667. 768. 815. 862	
császárvadász	169		
csatahajó	787	csütörtök	354
csendőr	812		

Kazalo tajnopisnih oznaka.

A.

admiral	916	atentat	437
Albanija	410	attaché	694
albanski (a o)	675	Austrija	131
asentovanje konja	843	automobil	662

B.

ban	983	bosanski (a o)	998
baraka	507	Bosna	370
barikada	710	brahijum (pomoćnica)	313
bataljun	139	brigada	285
bilježnik	817	brod	816
bitka	796	brodovije	333, 719
bitnica	145	broj	893
bjegunac	562	brzojav	518
bojni brod	787	brzojavka	765
bolničkijivnica	867		

C.

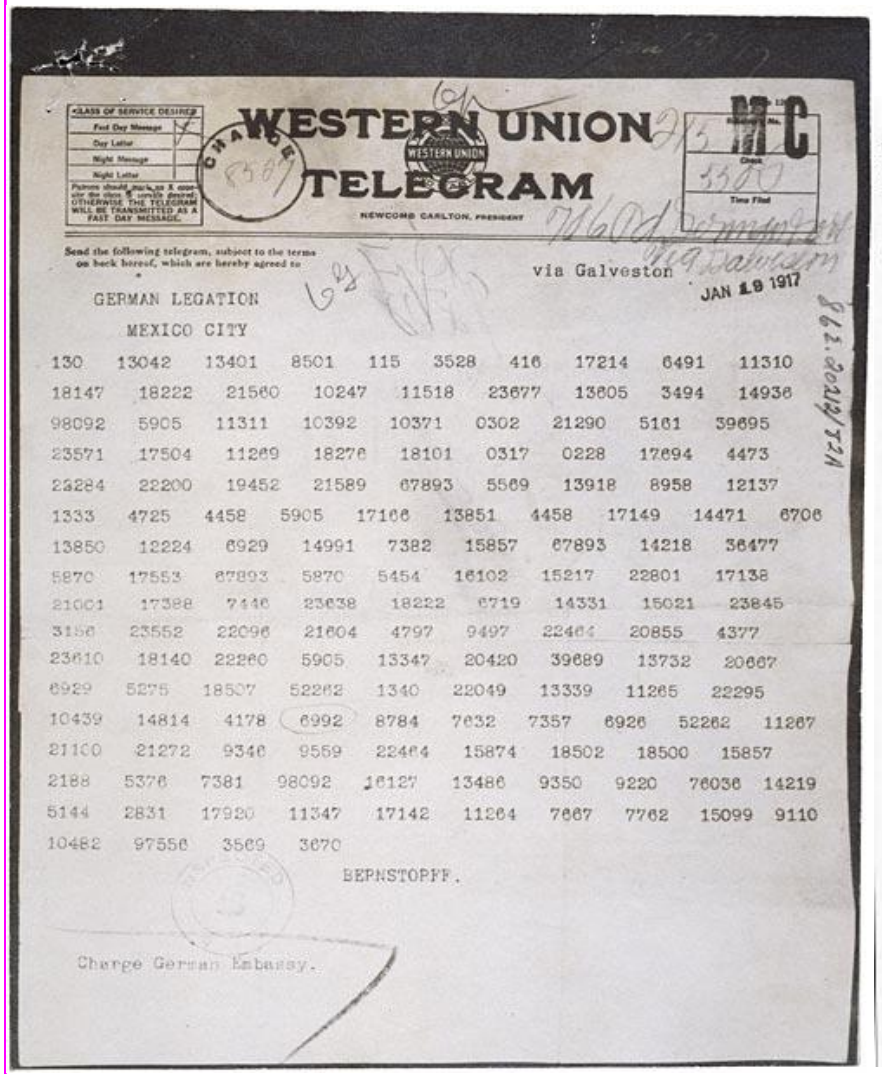
carski lovac	169	c. i. kr. (ces. i kralj.) 613. 653. 762. 804. 854. 904	
cesarsko kraljevski ministar za zemaljsku obranu	381	Crnagora	982
c. kr. (ces. kralj.) 564. 633. 667. 768. 815. 862		crnogorski	753

Č.

čamac	834	četna divizija	903
čardak	729	četno tielo	959
čas	879	četrnajsti	150
častnik	215	četujuća odvojka (četovnica)	614
častnički služak	933	četvrtak	354
četa	945	četvrti	418
četna bolnica	610		

A „Háromjegyű rejtjelkulcs" német, magyar és horvát nyelvű első oldalai

Zimmermann Telegram, 19 January 1917



WESTERN UNION TELEGRAM

NEWCOMB CARLTON, PRESIDENT

Send the following telegram, subject to the terms on back hereof, which are hereby agreed to

via Galveston

JAN 19 1917

GERMAN LEGATION

MEXICO CITY

130 13042 13401 8501 115 3528 416 17214 6491 11310
18147 18222 21560 10247 11518 23677 13605 3494 14936
98092 5905 11311 10392 10371 0302 21290 5161 39695
23571 17504 11269 18276 18101 0317 0228 17694 4473
23284 22200 19452 21589 67893 5569 13918 8958 12137
1333 4725 4458 5905 17166 13851 4458 17149 14471 6706
13850 12224 6929 14991 7382 15857 67893 14218 36477
5870 17553 67893 5870 5454 16102 15217 22801 17138
21001 17388 7446 23638 18222 6719 14331 15021 23845
3156 23552 22096 21604 4797 9497 22464 20855 4377
23610 18140 22260 5905 13347 20420 39689 13732 20667
6929 5275 18507 52262 1340 22049 13339 11265 22295
10439 14814 4178 6992 8784 7632 7357 6926 52262 11267
21100 21272 9346 9559 22464 15874 18502 18500 15857
2188 5376 7381 98092 16127 13486 9350 9220 76036 14219
5144 2831 17920 11347 17142 11264 7667 7762 15099 9110
10482 97556 3569 3670

BERNSTORFF.

Charge German Embassy.

TELEGRAM RECEIVED.

FROM 2nd from London # 5747.

"We intend to begin on the first of February unrestricted submarine warfare. We shall endeavor in spite of this to keep the United States of America neutral. In the event of this not succeeding, we make Mexico a proposal of alliance on the following basis: make war together, make peace together, generous financial support and an understanding on our part that Mexico is to reconquer the lost territory in Texas, New Mexico, and Arizona. The settlement in detail is left to you. You will inform the President of the above most secretly as soon as the outbreak of war with the United States of America is certain and add the suggestion that he should, on his own initiative, invite Japan to immediate adherence and at the same time mediate between Japan and ourselves. Please call the President's attention to the fact that the ruthless employment of our submarines now offers the prospect of compelling England in a few months to make peace." Signed, ZIMMERMANN.

Jaroslav Hašek:

Švejk: Egy derék katona kalandjai a világháborúban

A DICSŐSÉGES CSIHI-PUHI 1

- Sie, Kadett - mondta Ságner kapitány -, amíg nem kapott rá engedélyt, hogy beszéljen, addig hallgasson, mert magát nem kérdezte senki. Különben is, maga aztán átkozottul okos katona. **Éppen bizalmas információkat akarok közölni, és maga mindent beír a noteszába**. Ha elveszti azt a noteszt, hadbíróság elé kerül.

Biegler kadétnak mindennek tetejébe megvolt még az a rossz szokása, hogy mindig ki akarta magyarázni magát, hogy ő csak jót akart.

- Jelentem alássan, kapitány úr - felelte -, még a noteszom esetleges elvesztése esetén sem fejtheti meg senki se, hogy mit írtam, mert én gyorsírással jegyzek mindent, és az én rövidítéseimet rajtam kívül senki sem tudja elolvasni. Az angol rendszerű gyorsírást használom.

Mindenki megvetően nézett rá, Ságner kapitány legyintett, és folytatta előadását.

- Már említettem a **harctéri üzenetek sifrírozásának új módszerét**, és ha eddig talán érthetetlen volt az önök szemében, hogy miért hívták fel a figyelmüket éppen **Ludwig Ganghofer "Die Sünden der Väter"** című könyvének százhatvanegyedik oldalára, most megmagyarázhatom, uraim: ez a kulcsa az új rejtjeles módszernek, amely hadseregtörzsünk legújabb utasítása alapján lépett érvénybe. A legújabb módszert, amelyet mi is használni fogunk, **kiegészítő számmódszernek hívják**. Ezzel érvényüket vesztik azok az utasítások, amelyeket a múlt héten kaptak az ezredtörzstől a sifrírozásra és a rejtjelek megfejtésére vonatkozóan.

- Erzherzog Albrecht-system - morogta maga elé a stréber kadét - 8922-R, a Gronfeld-rendszerből átvéve.

A DICSŐSÉGES CSIHI-PUHI 2

- Az új módszer **rendkívül egyszerű** - zengett a kapitány hangja a vagonban -, személyesen vettem át az ezredes úrtól a második kötetet és az információkat... Ha például a következő parancsot akarják hozzánk intézni:
"Auf der Kote 228 Maschinengewehrfeuer links richten",
akkor, uraim, a következő szöveget kapjuk:
"Sache - mit - uns - das - wir - aufsehen - in - die - versprachen - die - Martha - dich - das - ängstlich - dann - wir - den - wir - Dank - wohl - Regiekollegium - Ende - wir - versprachen - wir - gebessert - versprachen - wirklich - denke - Idee - ganz - herrscht - Stimme - letzten."
Vagyis végtelenül egyszerűen, minden fölösleges kombináció nélkül. A stábtól telefonon a zászlóaljhoz, a zászlóaljtól telefonon a századhoz. Miután a parancsnok felvette ezt a sifrírozott üzenetet, a **következő módon fejti meg**. Veszi a "Die Sünden der Väter" című könyvet, kinyitja a százhatvanegyedik oldalon, és a szemközti oldalon, vagyis a százhatvanadikon, elkezdi felülről keresni a "Sache" szót. Tessék, uraim. A százhatvanadik oldalon a "Sache" szó először mint az ötvenkettedik szó fordul elő, tehát a parancsnok a szemközti oldalon, a százhatvanegyediken, megkeresi felülről az ötvenkettedik betűt. Tessék megfigyelni, hogy az egy "A" betű. Az üzenet következő szava: "mit". A százhatvanadik oldalon ez a hetedik szó, ez megfelel a százhatvanegyedik oldal hetedik betűjének, vagyis az "u" betűnek. Azután következik az "uns", vagyis, jól figyeljék meg, kérem, a nyolcvannyolcadik szó, ami a szemközti, százhatvanegyedik oldal nyolcvannyolcadik betűjének, az "f" betűnek felel meg, és így már meg is fejtettünk annyit, hogy "Auf". Ily módon folytatjuk, amíg világosan előttünk áll a parancs: **"A 228-as magaslaton gépfegyvertüzet balra irányíts."** Rendkívül elmés, uraim, igen egyszerű, és lehetetlen megfejteni a kulcs nélkül, ami nem más, mint Ludwig Ganghofer: "Die Sünden der Väter" című könyvének százhatvanegyedik oldala.

A DICSŐSÉGES CSIHI-PUHI - 3

Mindannyian némán bámulták a szerencsétlen oldalakat, s valahogy gondterhelten tűnődtek rajtuk. Egy ideig csend volt, aztán Biegler kadét egyszerre csak ijedten felkiáltott:

- Herr Hauptmann, ich melde gehorsam: Jesus Maria! Es stimmt nicht!

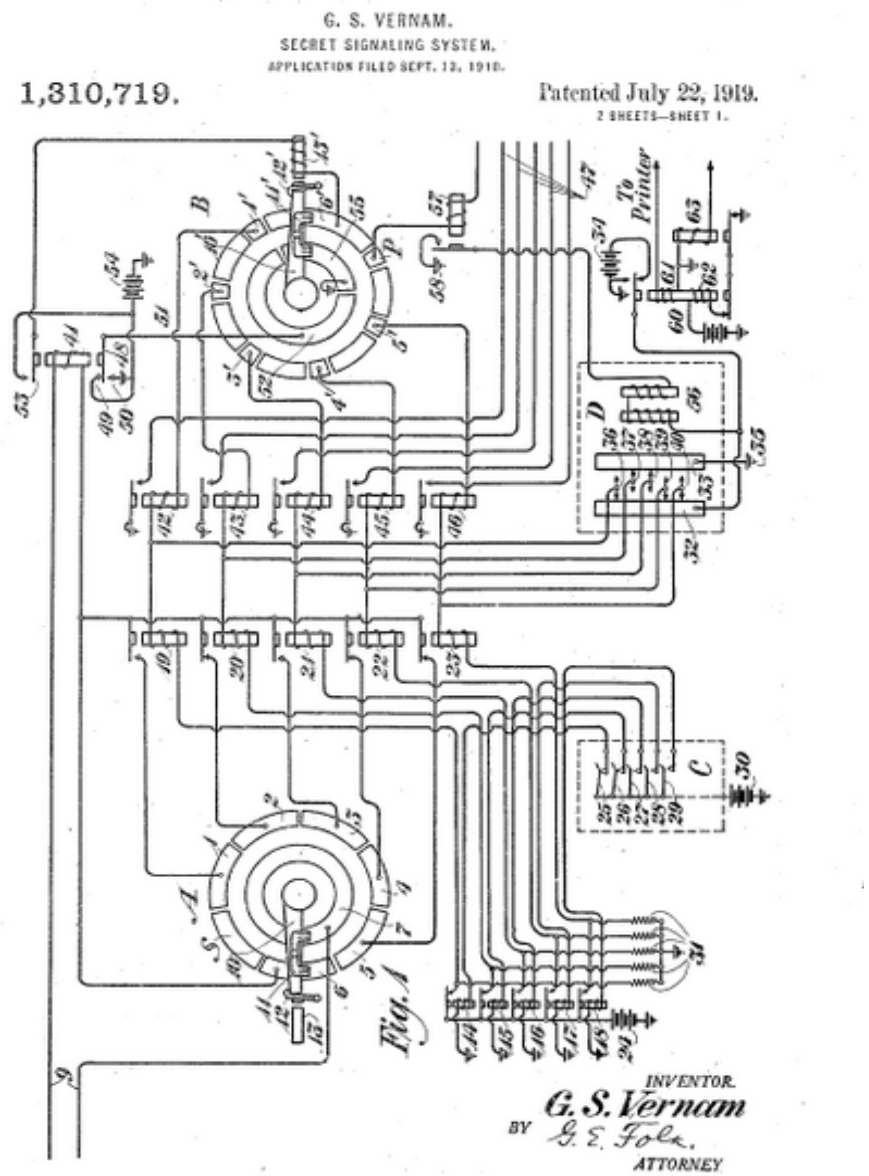
És valóban igen rejtélyes volt a dolog.

Hiába erőlködtek, ahogy csak bírtak, Ságner kapitányon kívül senki se találta meg a százhatvanadik oldalon az említett szavakat s a szemközti, százhatvanegyedik oldalon, amely a kulcsot jelentette volna, az említett szavaknak megfelelő betűket.

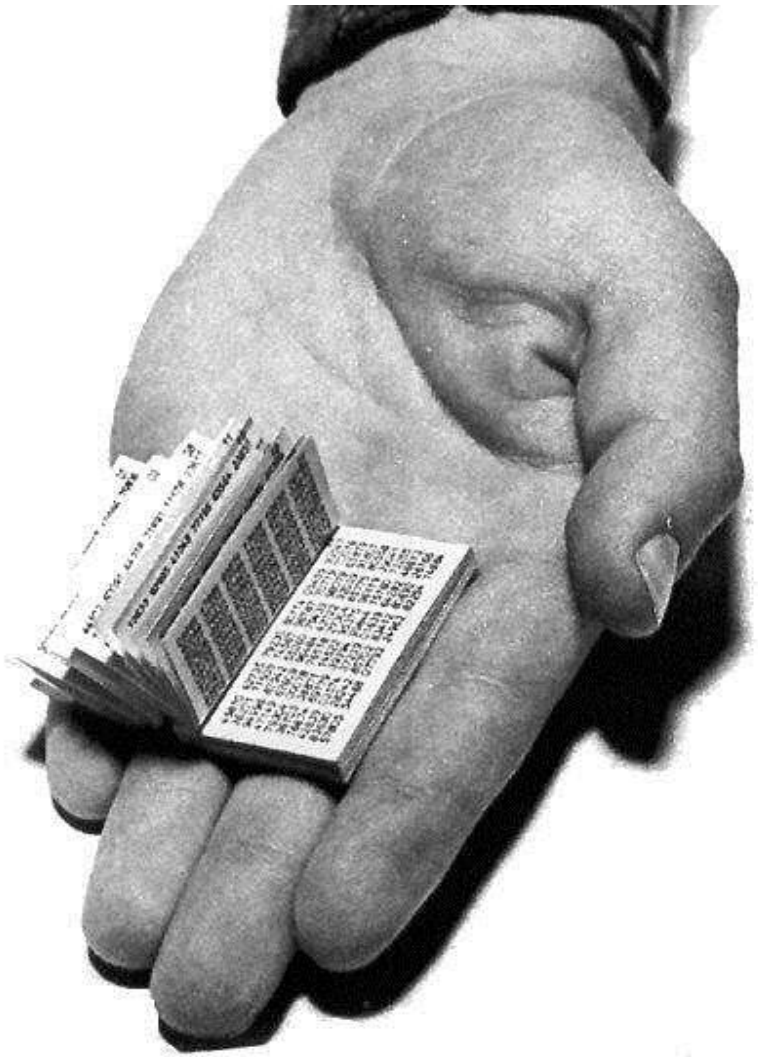
- Meine Herren - dadogta Ságner kapitány, miután meggyőződött róla, hogy Biegler kadét kétségbeesett kiáltása megfelel az igazságnak -, mi történt itt? Az én Ganghoferemben megvan és az önökében nincs meg?

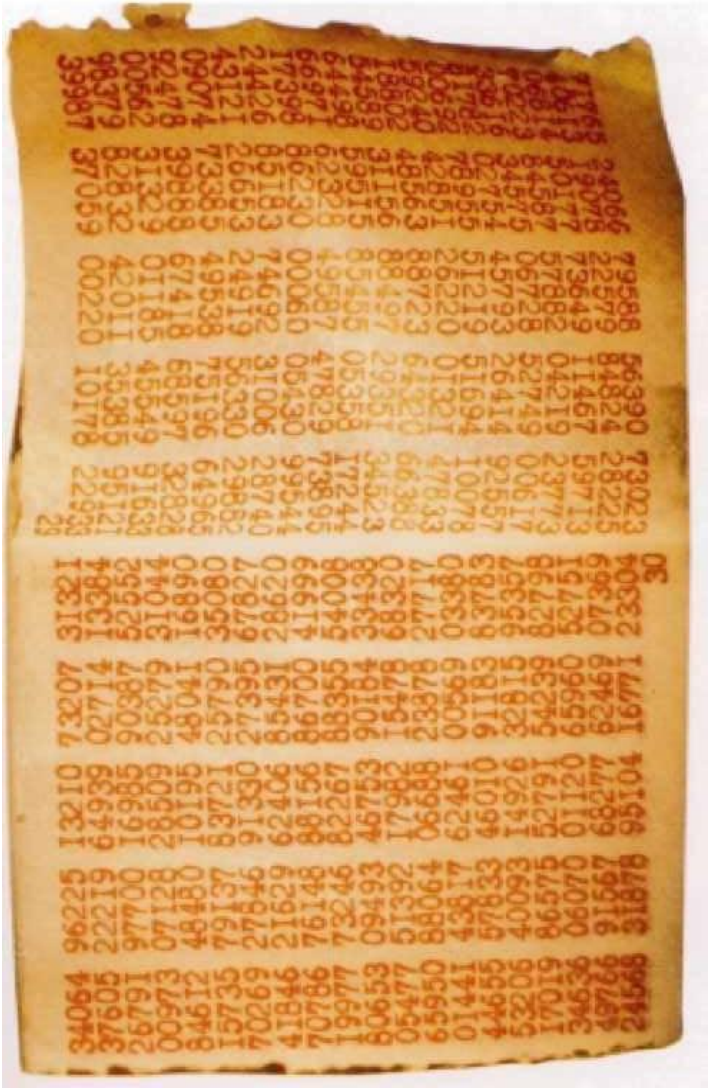
- Bocsánat, kapitány úgy - szólalt meg ismét Biegler kadét. - Szíves engedelmével felhívom a figyelmét arra, hogy **Ludwig Ganghofer regénye két kötetből áll.** Méltóztassék megtekinteni a címoldalt**: "Roman in 2 Bänden."**

This drawing shows Gilbert Vernam's original concept for a teletype encryption machine



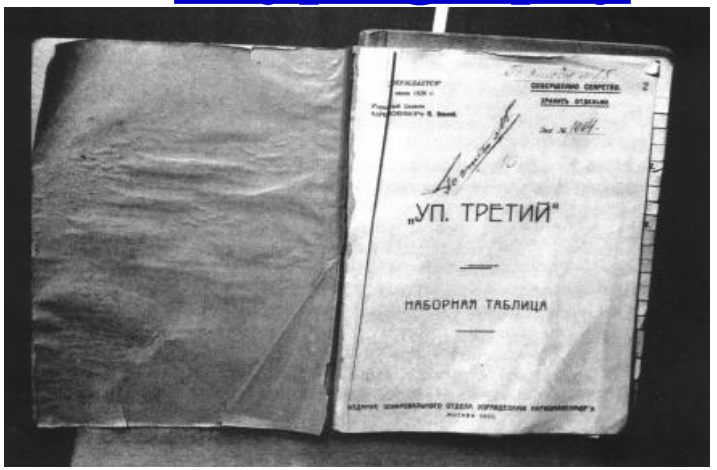
Historische OTPs für die Vernam-Verschlüsselung





The Soviet – Russian Cryptography

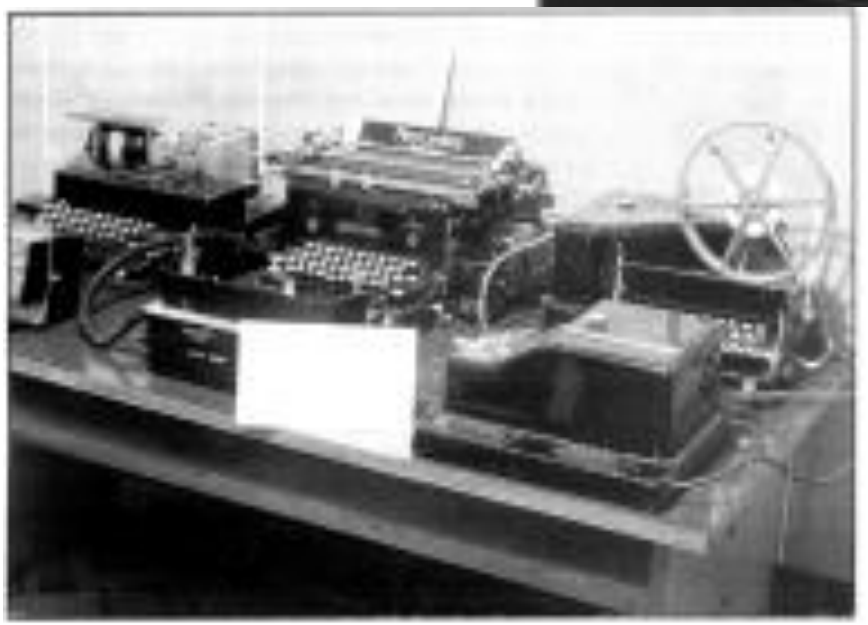
Code book of the Russian Czar.



Code books.

The Soviet Cyptography

Encryption Machine „KRIGA MALAJA”

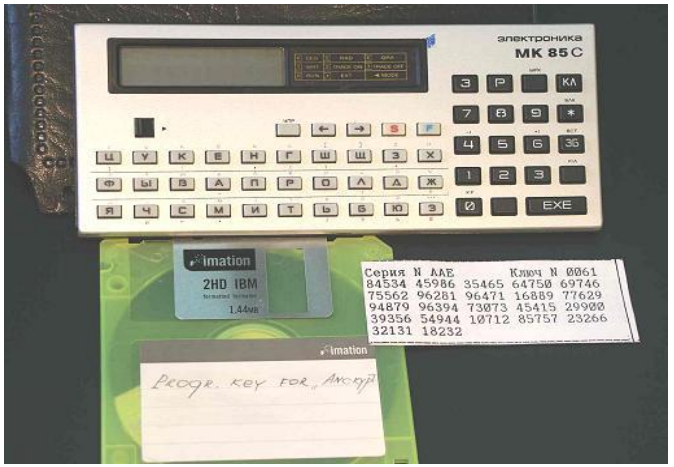


Encryption Machine „M-211”

Encryption Machine „M100”

The Soviet Cryptography

Ancrypt 2



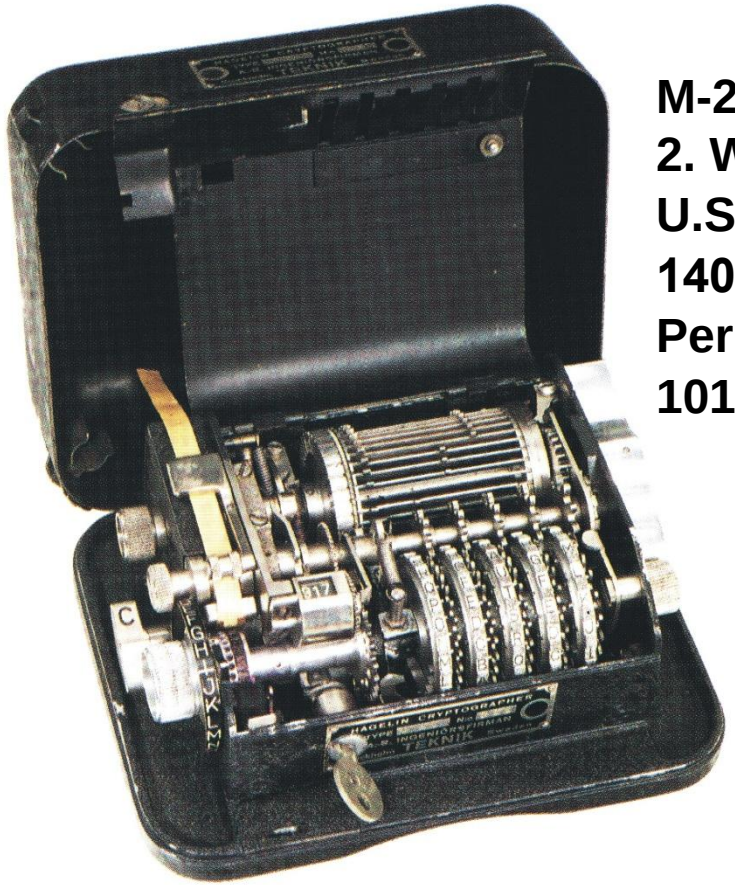
Ancrypt 5 / MK 85C

Ancrypt 512 / MK85C

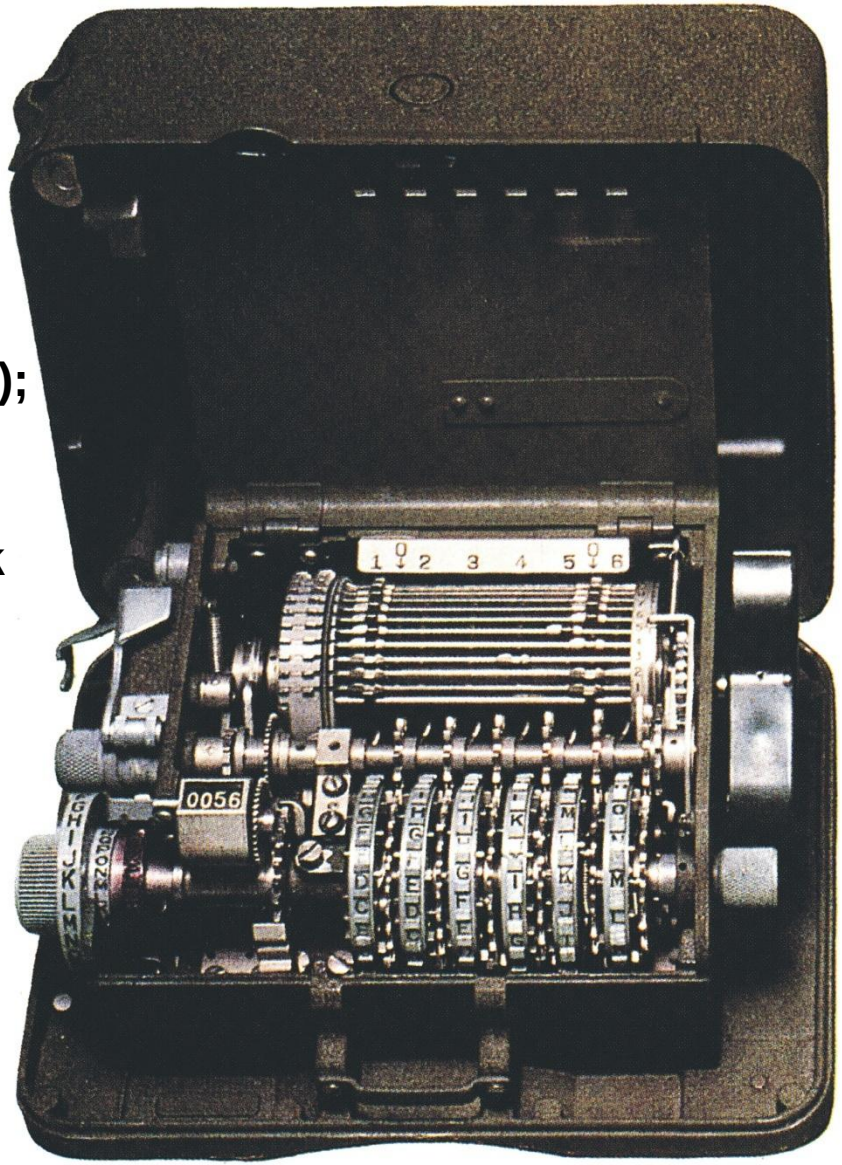
Mechanical Calculator

HAGELIN's CHIFFRIERMASCHINEN

Boris Hagelin; Stockholm, 1936;
Cryptographer C-36 (links);
Beaufort-Substitution,
Schlüssellänge: 3.900.225



M-209 (rechts);
2. Weltkrieg,
U.S. Army
140.000 Stück
Periode:
101.405.950



Nach:
F.L.Bauer:
Entzifferte
Geheimnisse

ROTOROS TIKOSITÓ GÉPEK

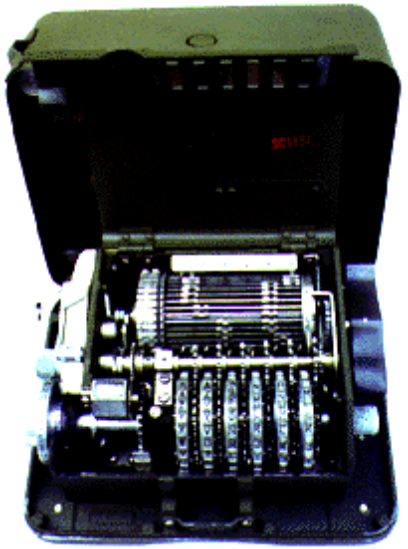
A ROTOROS mechanikus titkosító gépeket az 1930-s években fejlesztették ki taktikai üzenetek kódolására. A svéd M-209-B amerikai változata a CSP-1500 lett. Szalag-nyomtató kódoló-dekódoló szerkezet. Működése a reciprok behelyettesítő ábécé elvén alapszik: ettől egy standard betű szekvenciát egy fordított standard betűszekvenciaval szemben. E funkciót számos fogaskerék áttétellel valósítja meg úgy, hogy az aktív fogak száma változtatható. Először 1942 novemberében, az afrikai invázióban alkalmazták. Több mint 140.000-t gyártottak.

Hagelin M-209-B rotoros titkosító gépe,
1930, Svédország

(forrás: International Association for Cryptologic Research)

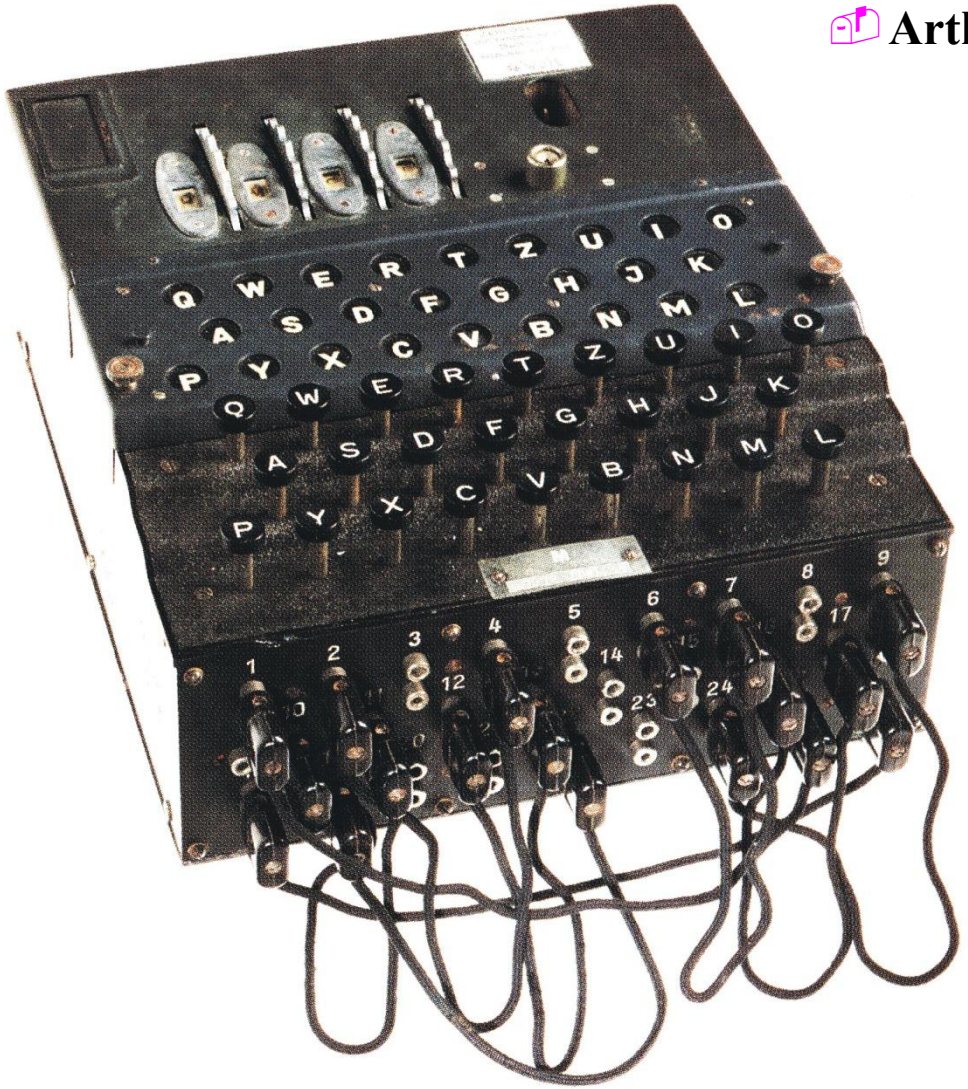
CSP-1500 rotoros titkosító gép
1940, US Army Signal Corp

(forrás: National Maritime Museum Association)

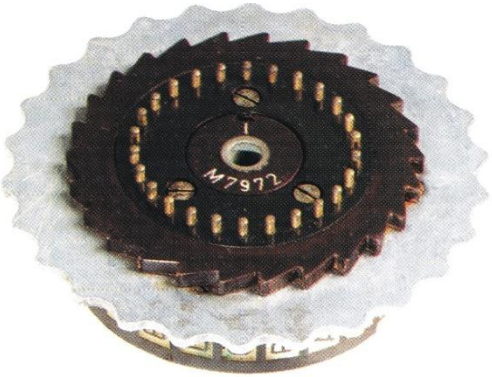


Az “ENIGMA” ROTOROS CHIFFRIER-GÉP

- **Arthur Scherbius, 1919** eredeti gépe;



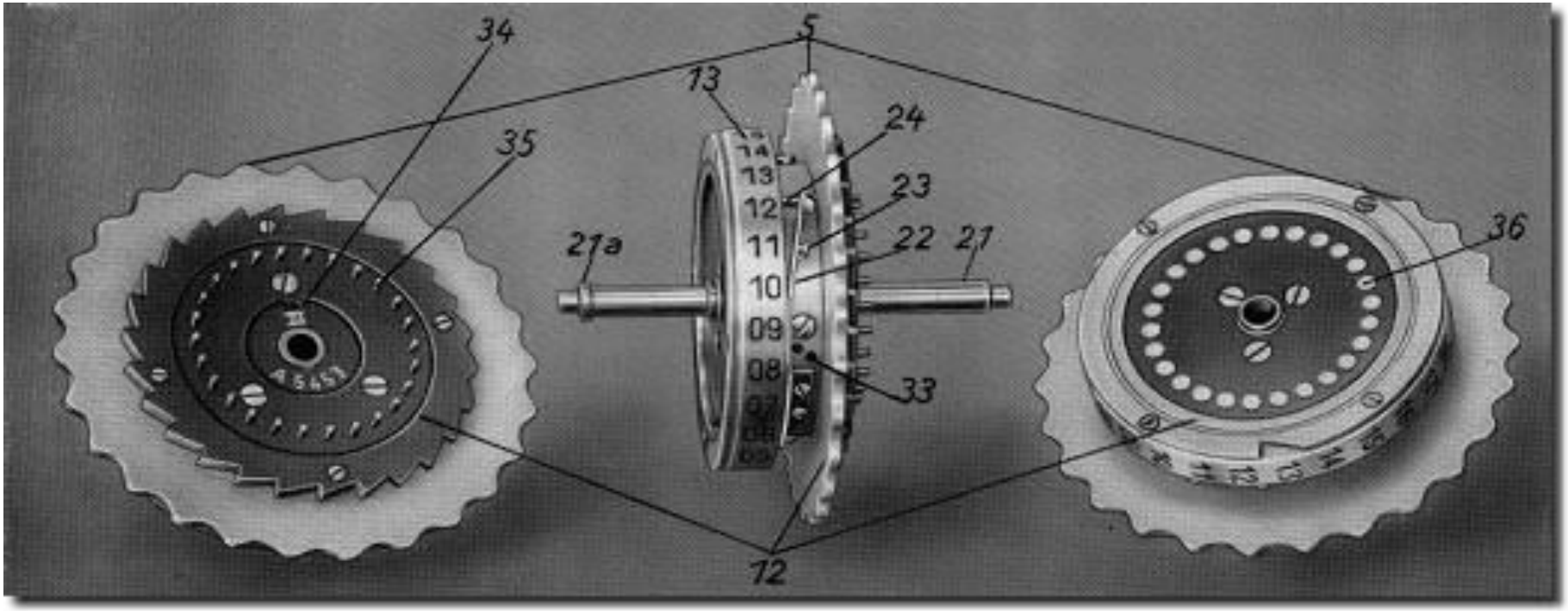
- **Az ENIGMA rotorjai**



Nach:F.L.Bauer:
Entzifferte Geheimnisse

The wheels of the ENIGMA

Die Räde von ENIGMA



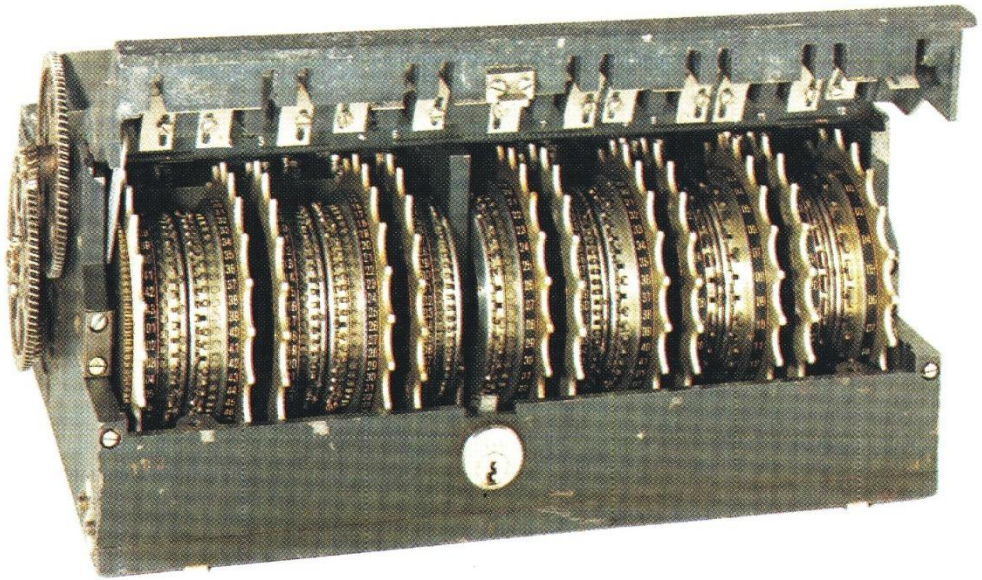
THE GERMAN ENIGMA

- Many variants was developed.
- Some variants was broken by:
  - Poles in 1930,
  - British in the World War II.
  - British and USA: the naval ENIGMA
- Question of an American officer
  - “If ever, we would have won the war, if we hadn’t read the ENIGMA?”
- The National Cryptologic Museum, NSA, USA

- Több variánsa volt kifejlesztve.
- A lengyelek 1930-ban, a britek a II. világháborúban már feltörték.
- Amerikai segítséggel a britek a „tengerészeti ENIGMA”-t is feltörték.
- Amerikai kérdés:
  „Megnyertük volna-e a háborút valaha is, ha nem tudjuk olvasni az ENIGMA-t”

CHIFFRIERGERÄTEN

- **Die UHR BOX, genannt bei alliierten** (rechts)**, diente dazu, die Steckerbrett-Verbindungen der ENIGMA zu ersetzen.**
- **Chiffrierfernschreibmaschine „Schüsselzusatz“ Lorenz SZ 42, C. Lorenz AG, Berlin, 1943** (links)**; Britischer Deckname „Tunny“. Gebrochen bei Briten mit COLOSSUS, der ersten elektronischen Großrechenanlage.**

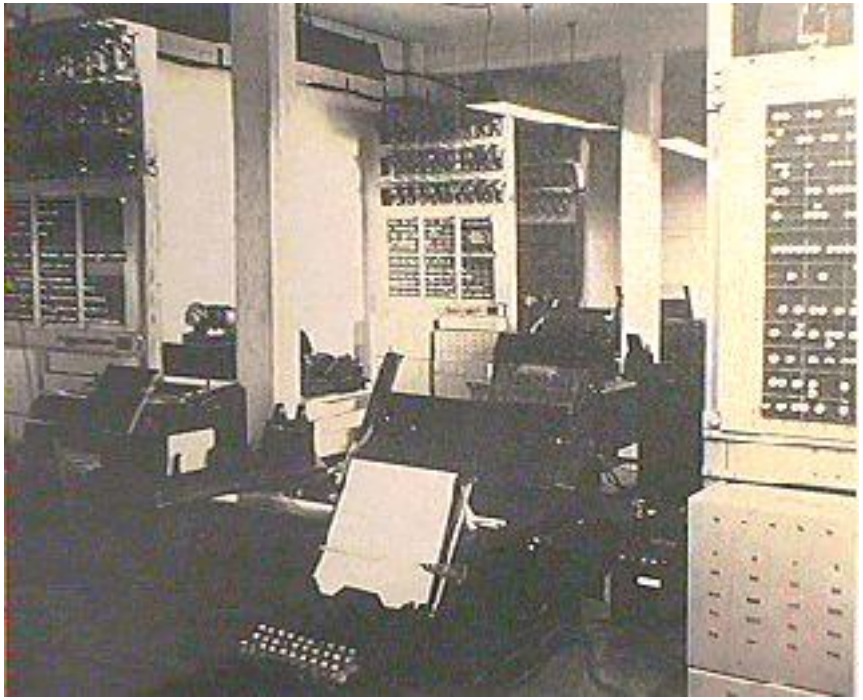


Nach:
F.L.Bauer:
Entzifferte
Geheimnisse

THE GERMAN LORENZ CIPHER SYSTEM

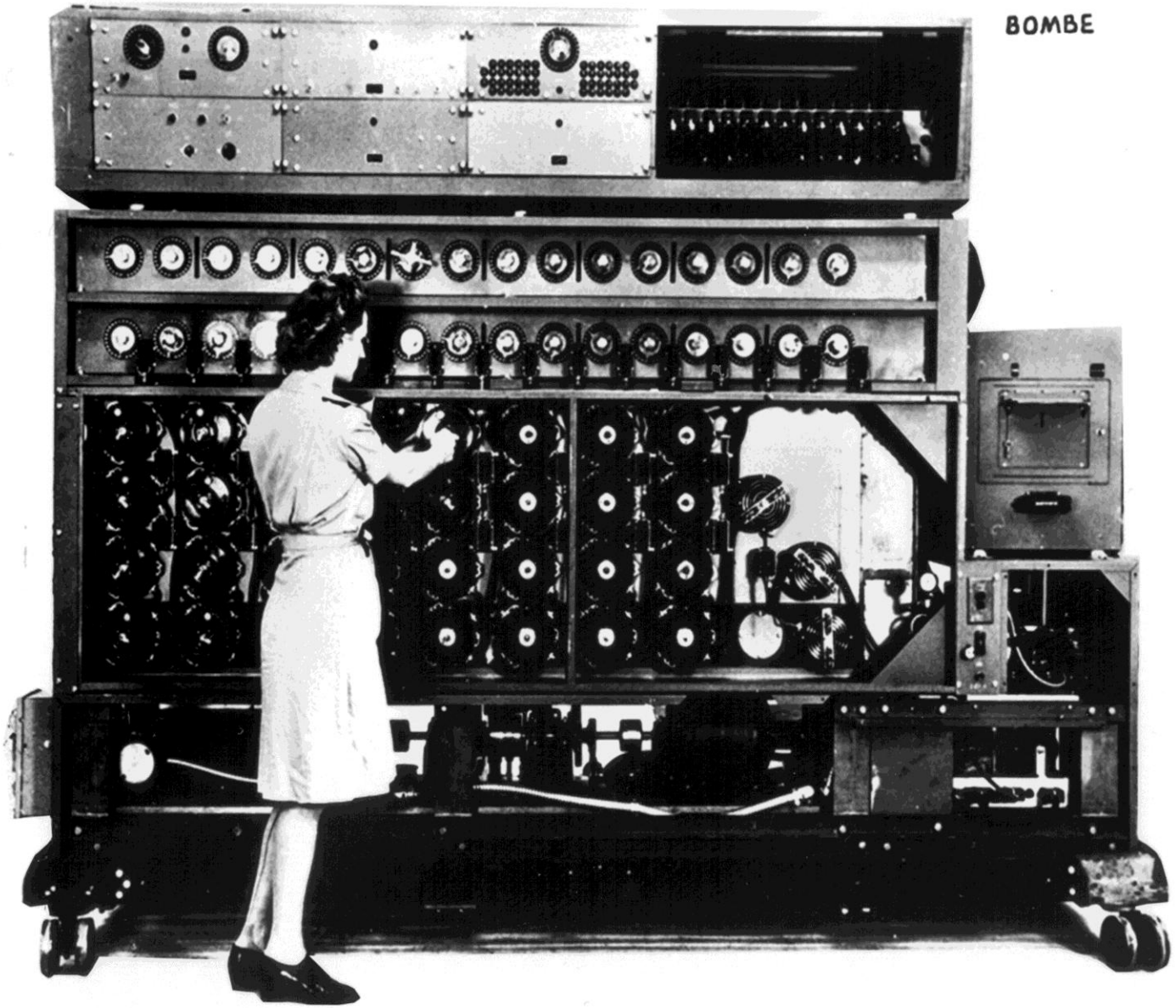
Bill Tutte (left) with
Tony Sale,
in about 1998

A **Tunny Machine**
Bill Tutte & Co.
Frank Morrell



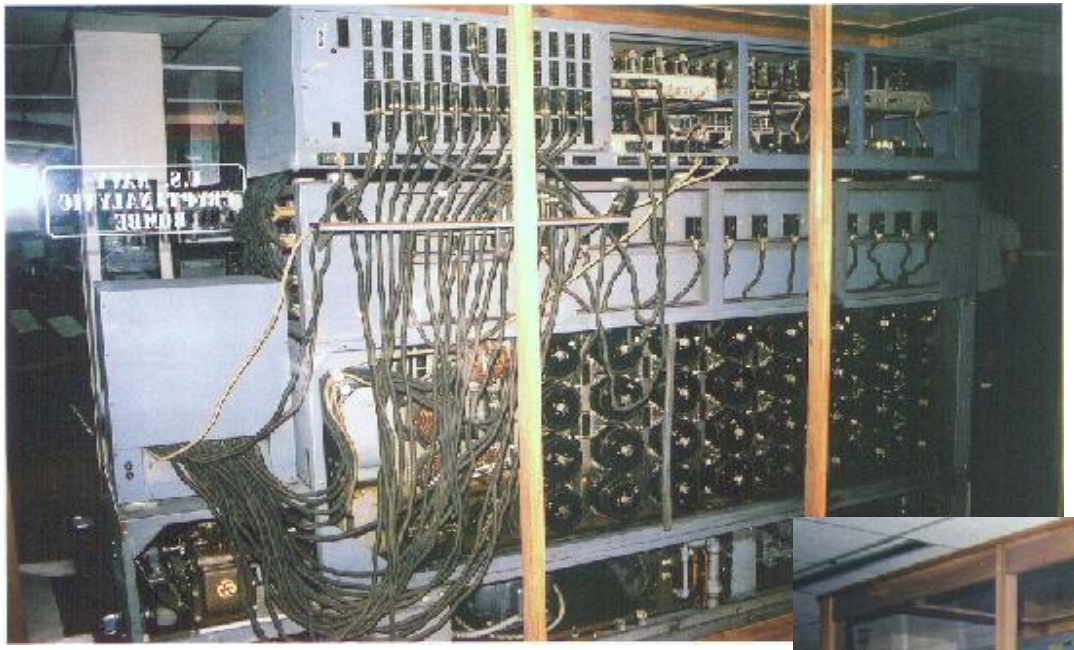
The **Lorenz company** designed a cipher machine based on the additive method for enciphering teleprinter messages invented in **1918** by **Gilbert Vernam** in America.

BLETCHLEY PARK: GC&CS



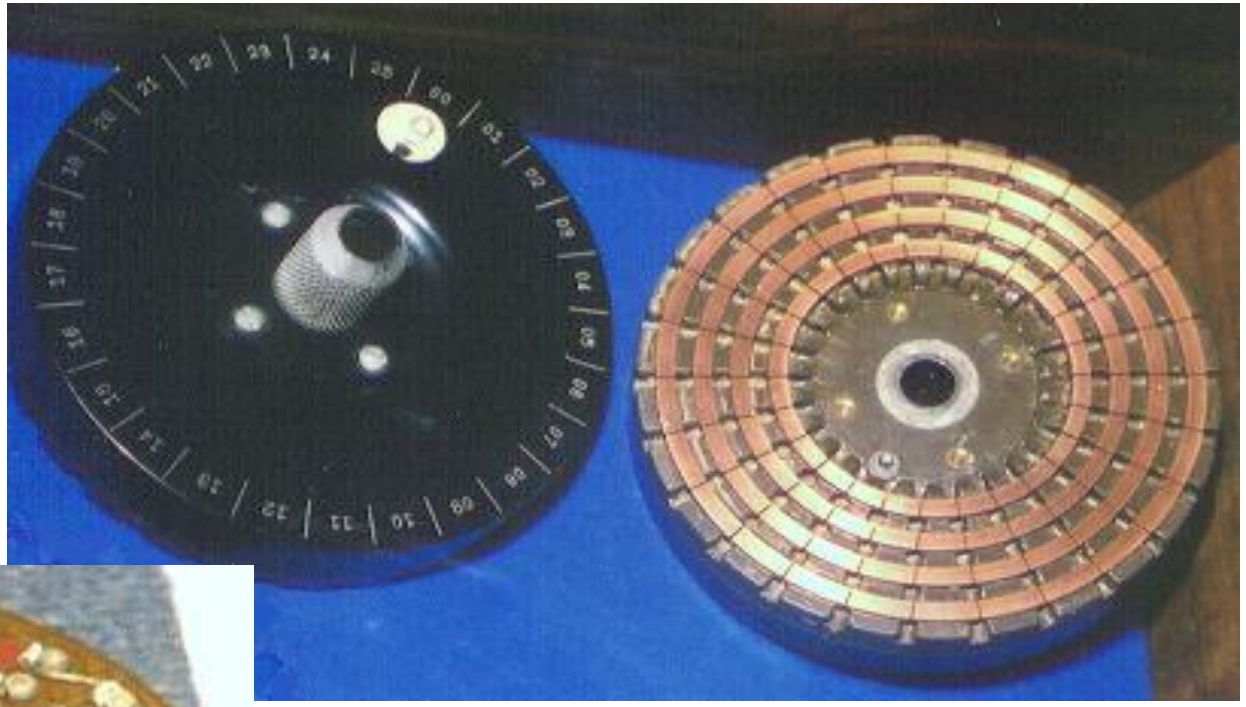
A WAVE with Bombe

WAVE :
Women Accepted for Voluntary Emergency Service



NCR Bombe as it is displayed in the National Cryptologic Museum

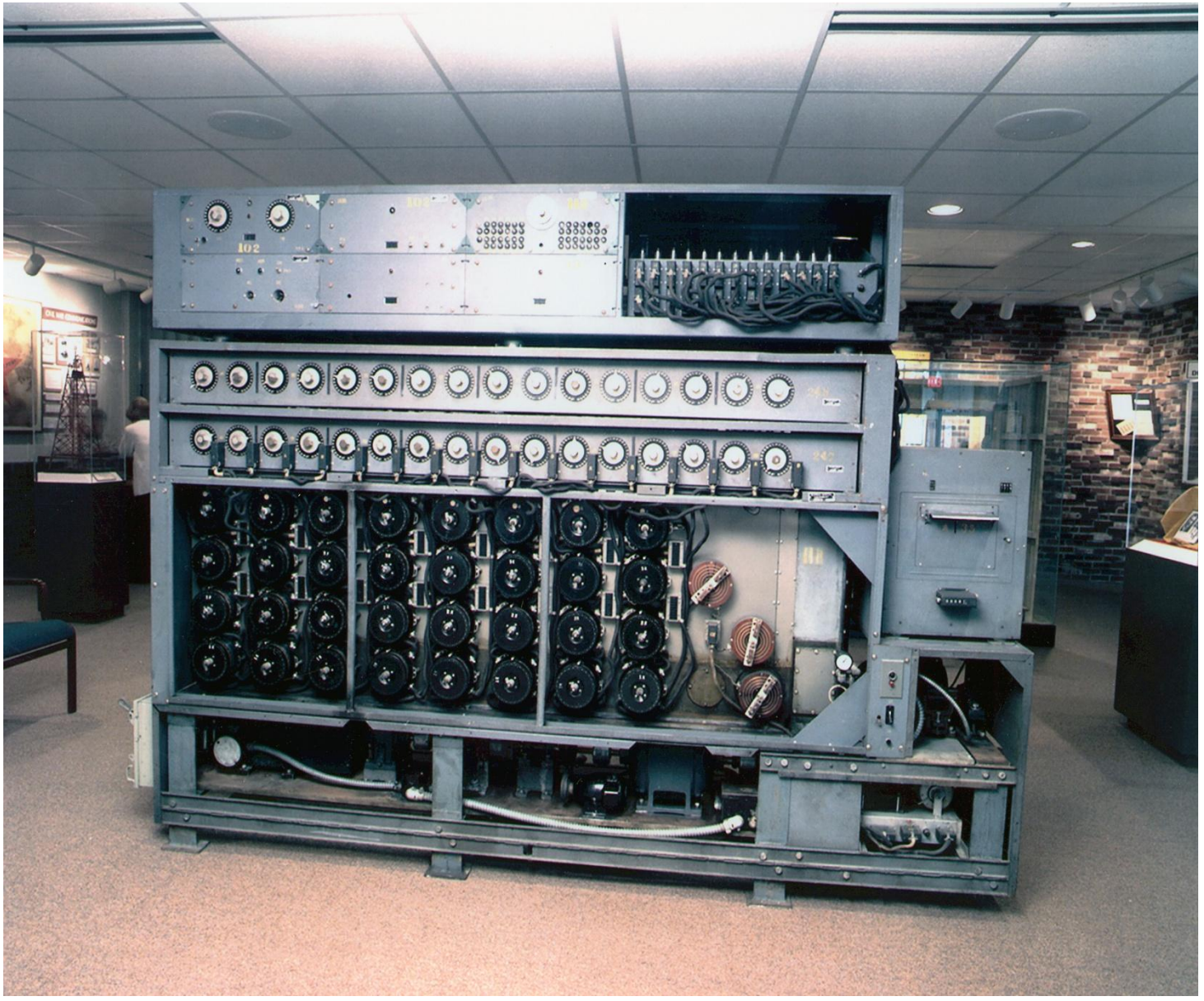
Actual bombe rotors



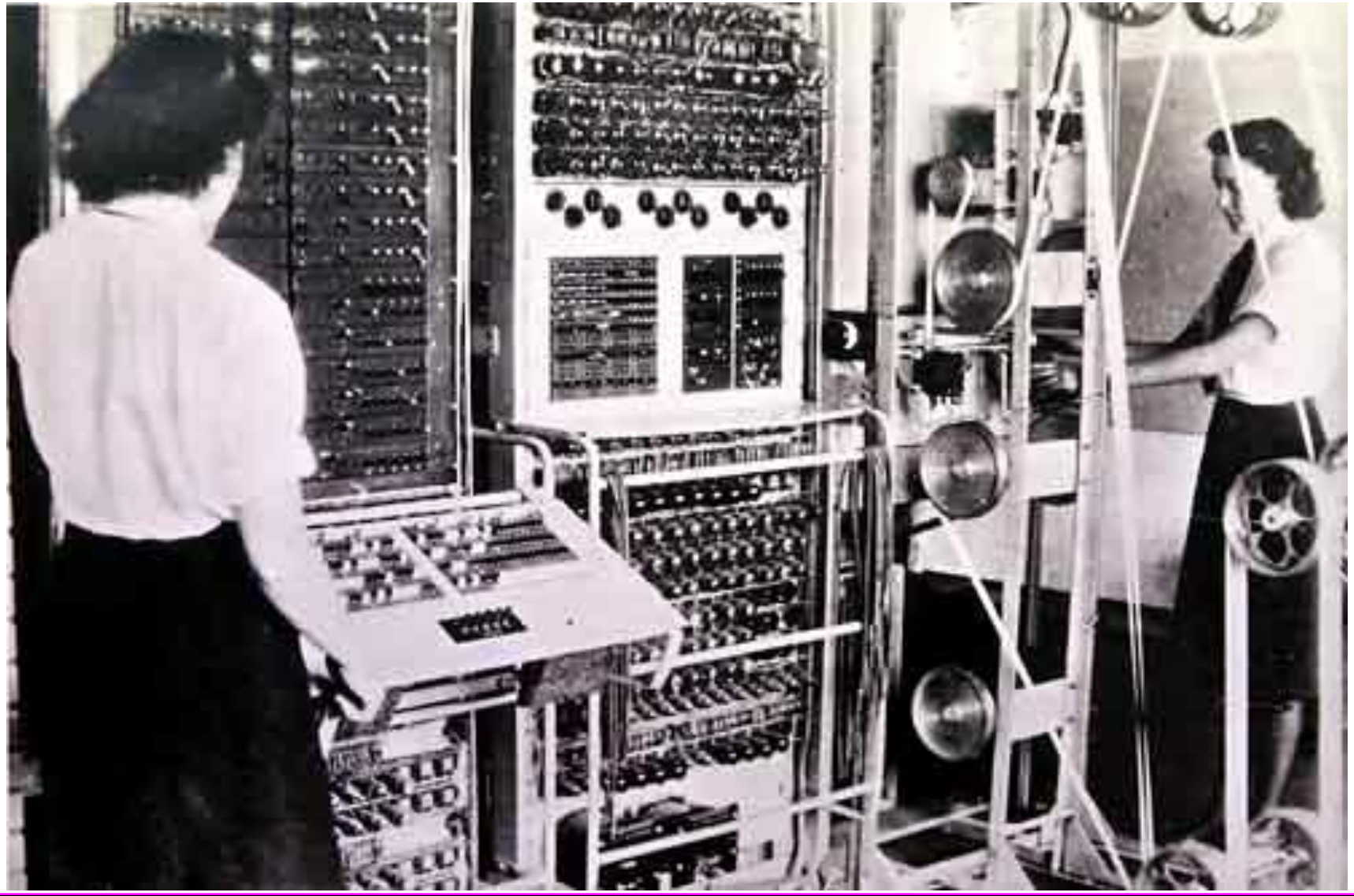
M9 Bombe Checking Machine

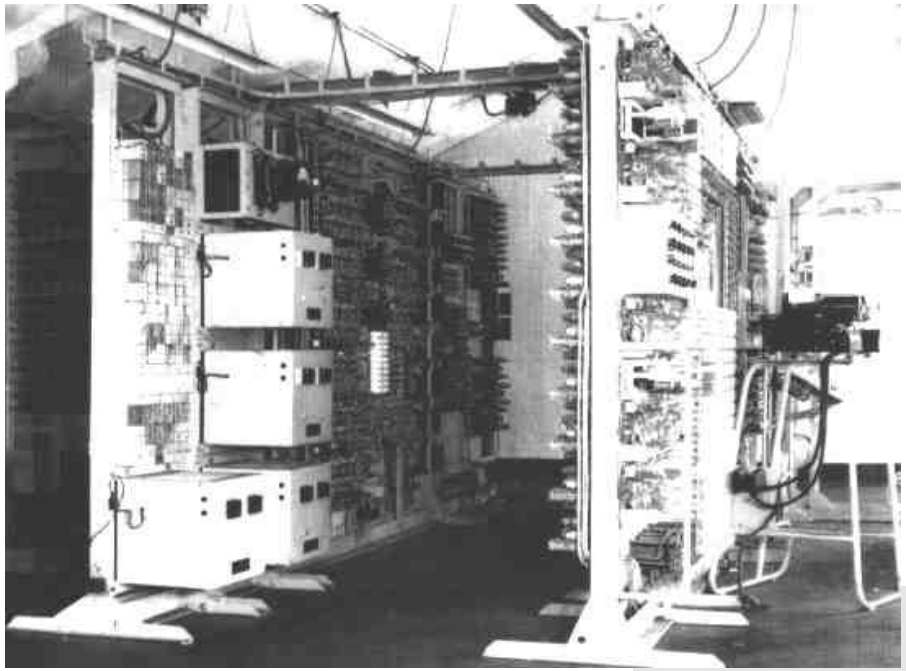
Joseph Desch, designer of the U.S. Navy bombe circa mid-1940's.

Bombe

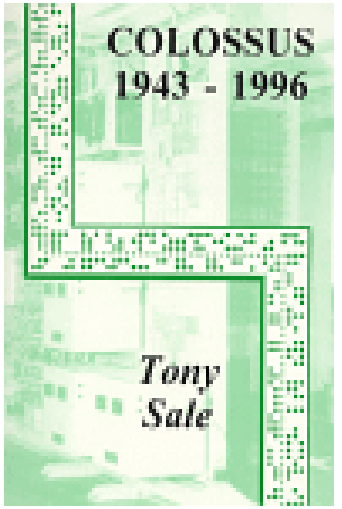


Colossus Computer at Bletchley Park (‘*Station X*’), Buckinghamshire , 1943

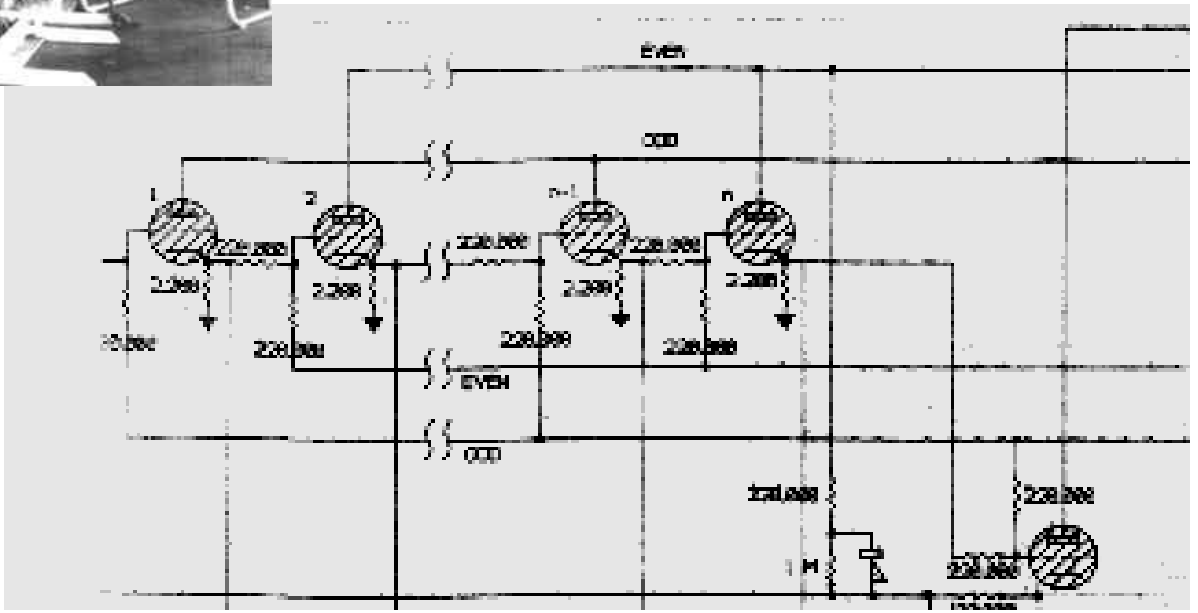




The Colossus



Thyratron rings.



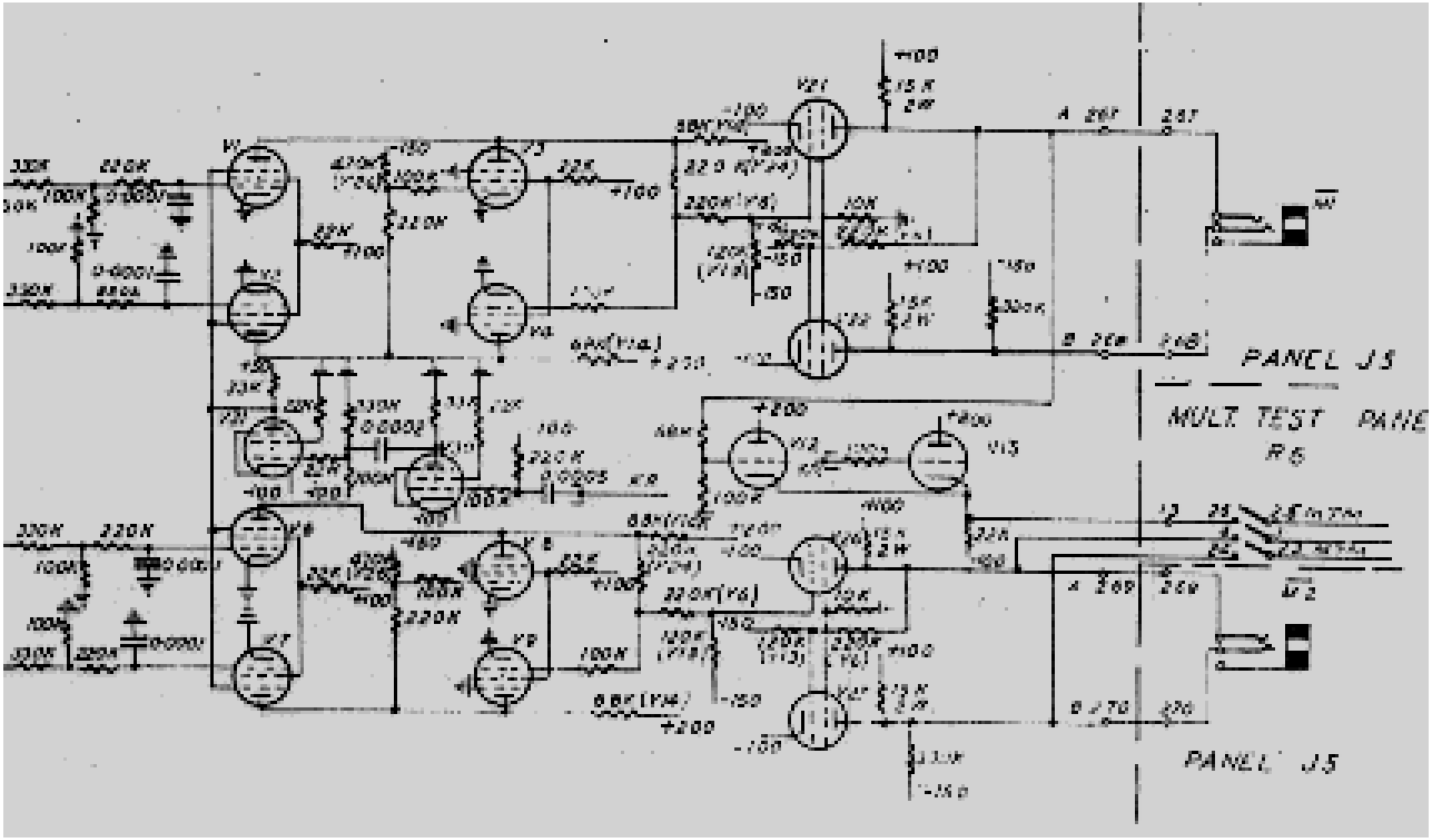
Colossus is not a stored-programme computer.

It is hard-wired and switch-programmed, just like ENIAC.

Because of its parallel nature it is very fast, even by today's standards.

THE SHIFT REGISTERS of COLOSSUS

This is thought to be the first recorded design or use of a shift register



BRITISCHE CHIFFRIERMASCHINE “TYPEX”

- Eine wesentlich verbesserte Kopie der Wehrmachts-ENIGMA mit drei Rotoren.
- Diente auch für Mechanischen Entzifferung deutscher ENIGMA-Sprüche, deren Schlüssel aufgedeckt war.

Nach:
F.L.Bauer:
Entzifferte
Geheimnisse

ÄQUIVALENTE U.S. ARMY CHIFFRIERGERÄTEN

Chiffriergerät „M-94“ der U.S. Army.

25 gravierten Aluminiumscheiben von 35 mm Durchmesser.

Einführt in Truppendienst unter dem Einfluß von Friedman.

1922-1942.

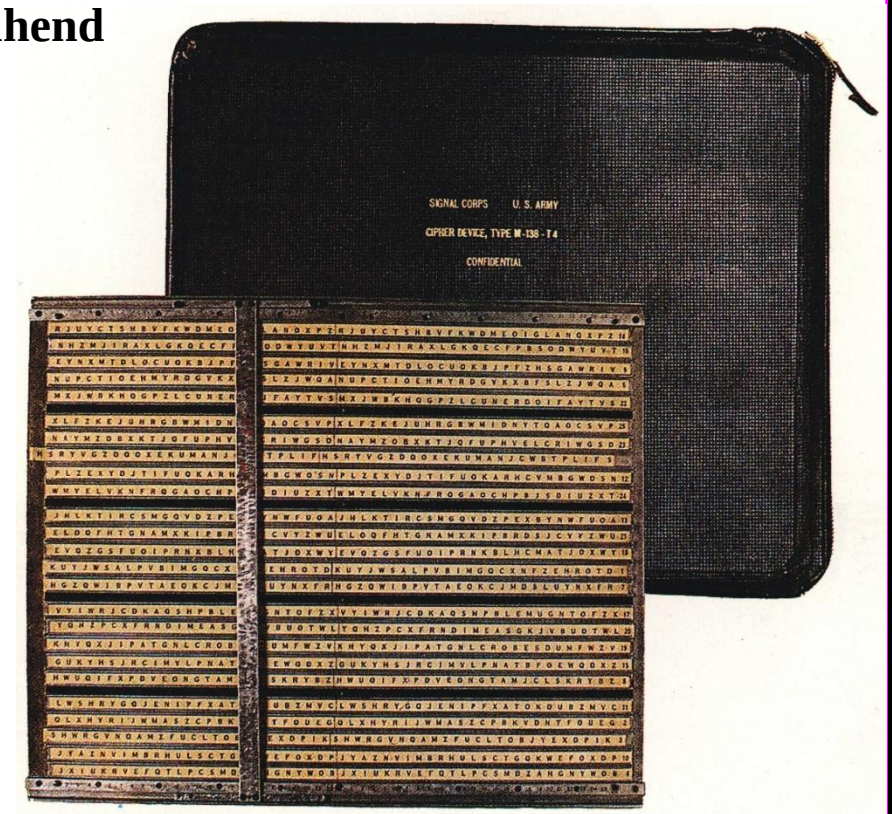
Geht auf die Vorbilder von Jefferson und Baseries zurück.

Nach:F.L.Bauer: Entzifferte Geheimnisse

Schiebergerät „M-138-T4“ der U.S. Army and U.S. Navy.

Benutzt in 2. Weltkrieg.

Auf einem Vorschlag von Parker Hitt (1914) beruhend



EGYSZER HASZNÁLATOS REJTJELZŐ KULCS

INDIVIDUELLER SCHLÜSSEL für EINMALIGEN GEBRAUCH

- A géppel irt betűk formája alapján feltételezhető, hogy orosz rejtjelző rendszer eleme.
- Ein Blatt aus ein Abreißblock.
- Die verwendeten Ziffern-Typen sind von der Art, wie sie auf russischen Schreibmaschinen vorkommen.

Nach: F. L. Bauer: Entzifferte Geheimnisse

The first 29 NAVAHO CODE SPEAKERS

Simon Singh: Kódkönyv: p.204.

The SIGABA and ECM

used by U.S. for high-level communications, was the only machine system used by any participant to remain completely unbroken by an enemy during World War II. The Germans referred to it as the "Big" machine.

The National Security Agency

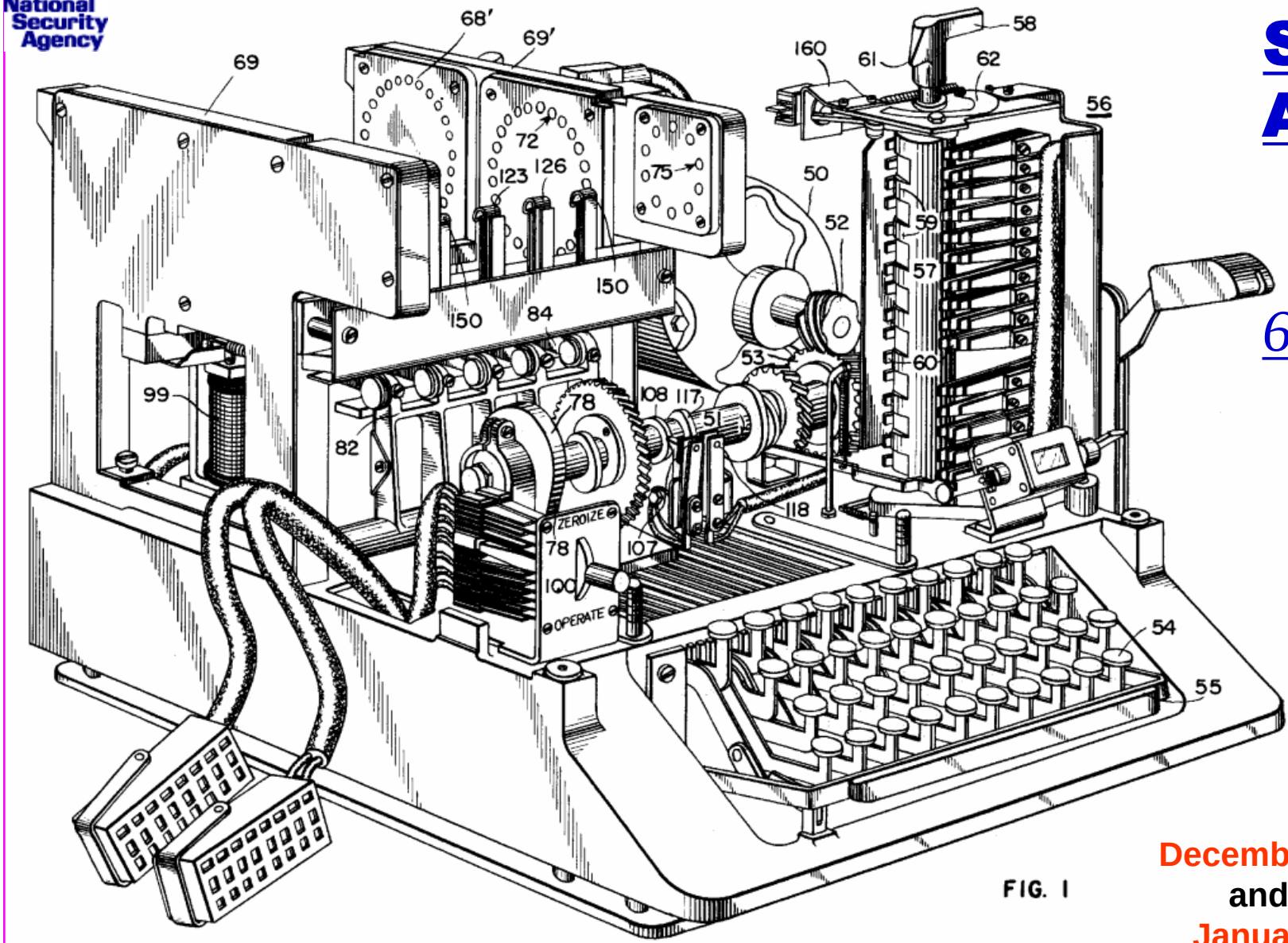


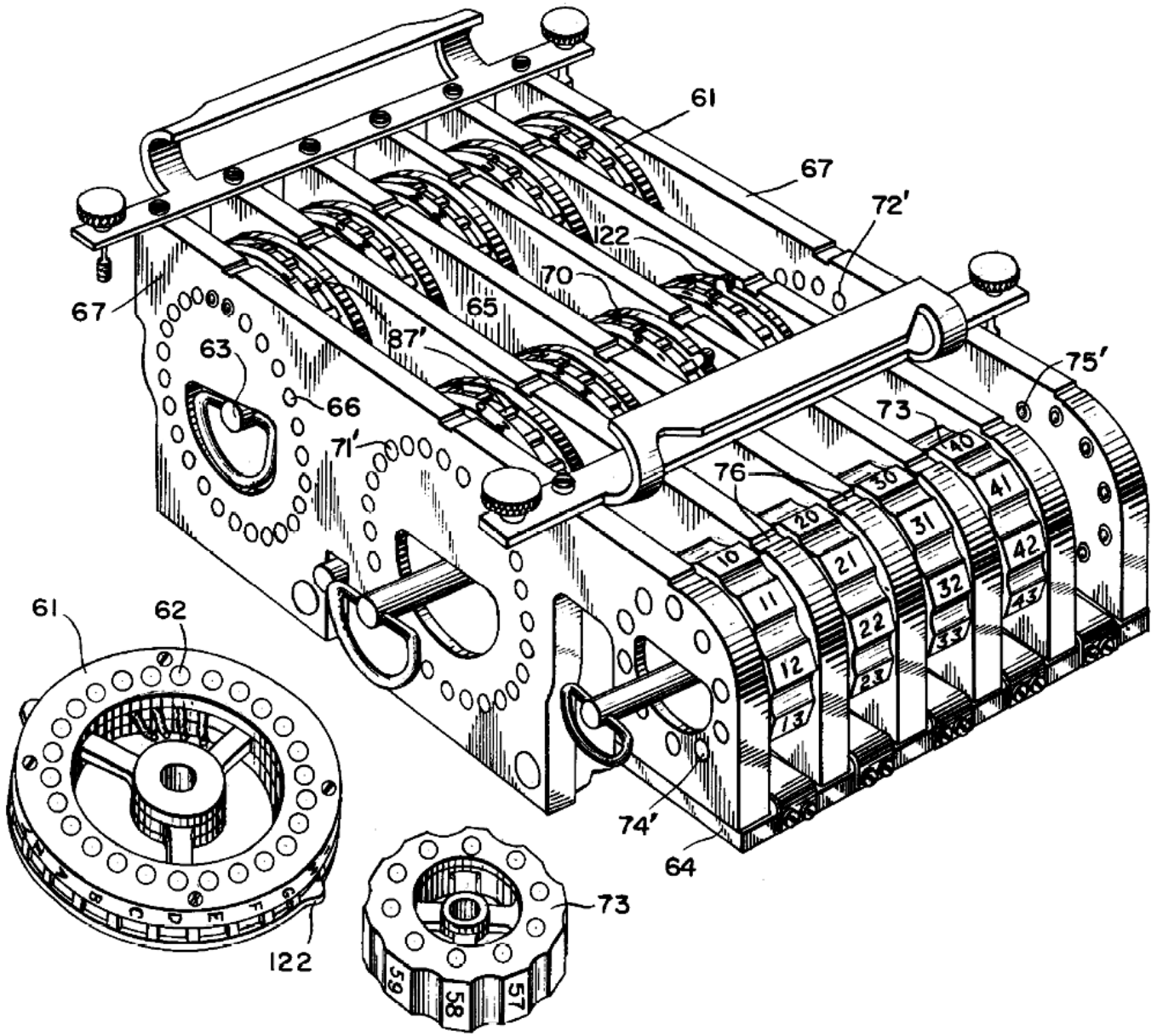
FIG. 1

SIGAB

AUnited States Patent 6,175,625

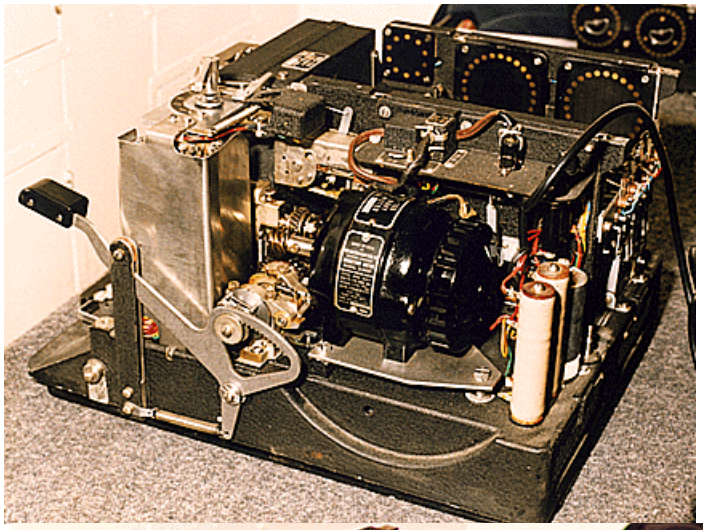
Filed for on December 15, 1944, and granted on January 16, 2001.

The SIGABA's Rotor Cage and Rotors.



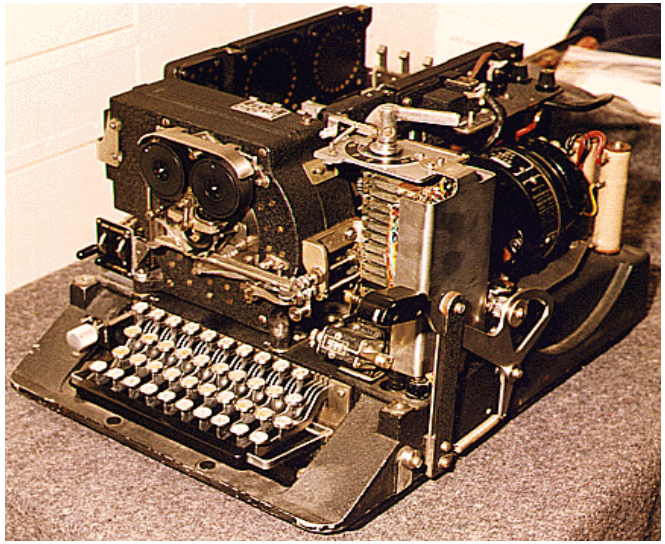
The National Security Agency

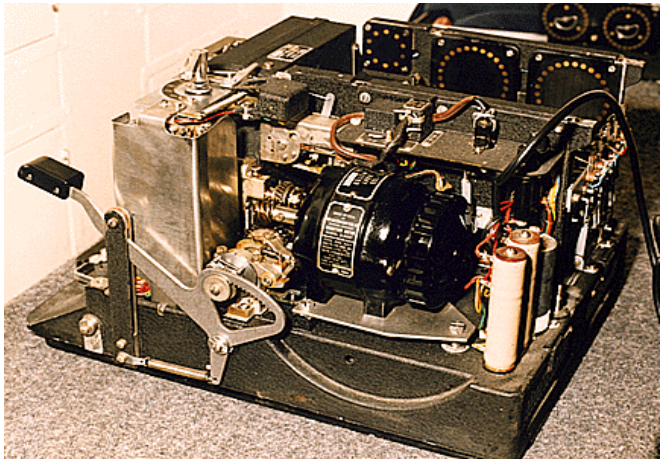
Electronic Cipher Machine (ECM) Mark II CSP 889/2900 or SIGABA or M-134-C, or CSP-889

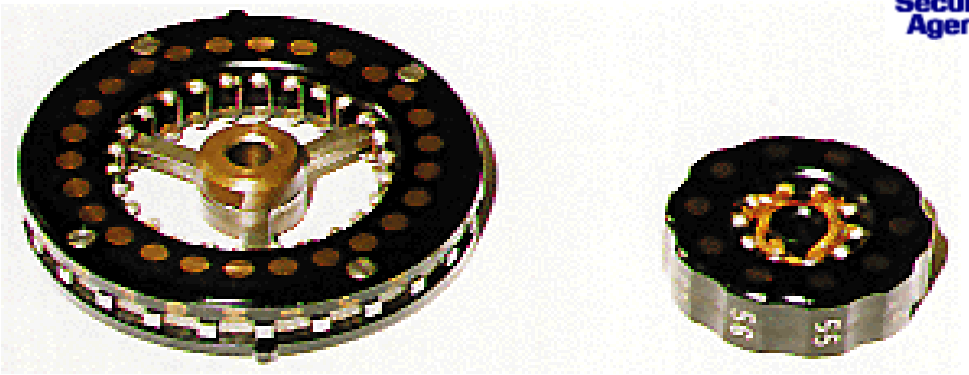


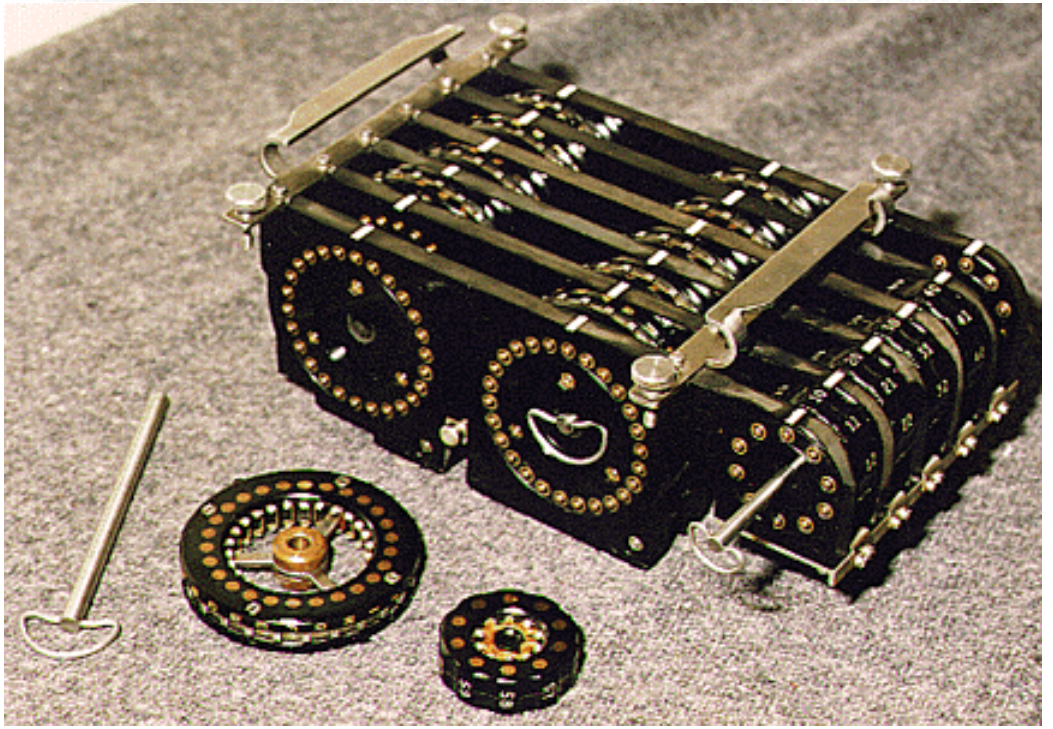
ECM: Electronic Cipher Machine

The National Security Agency



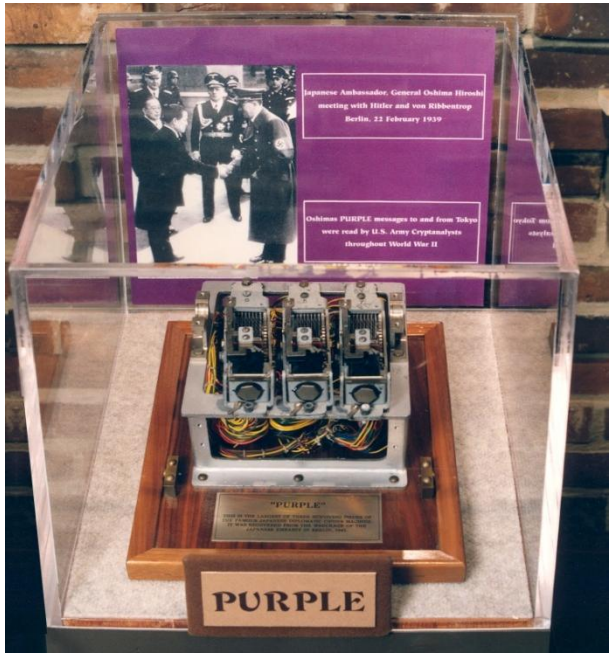


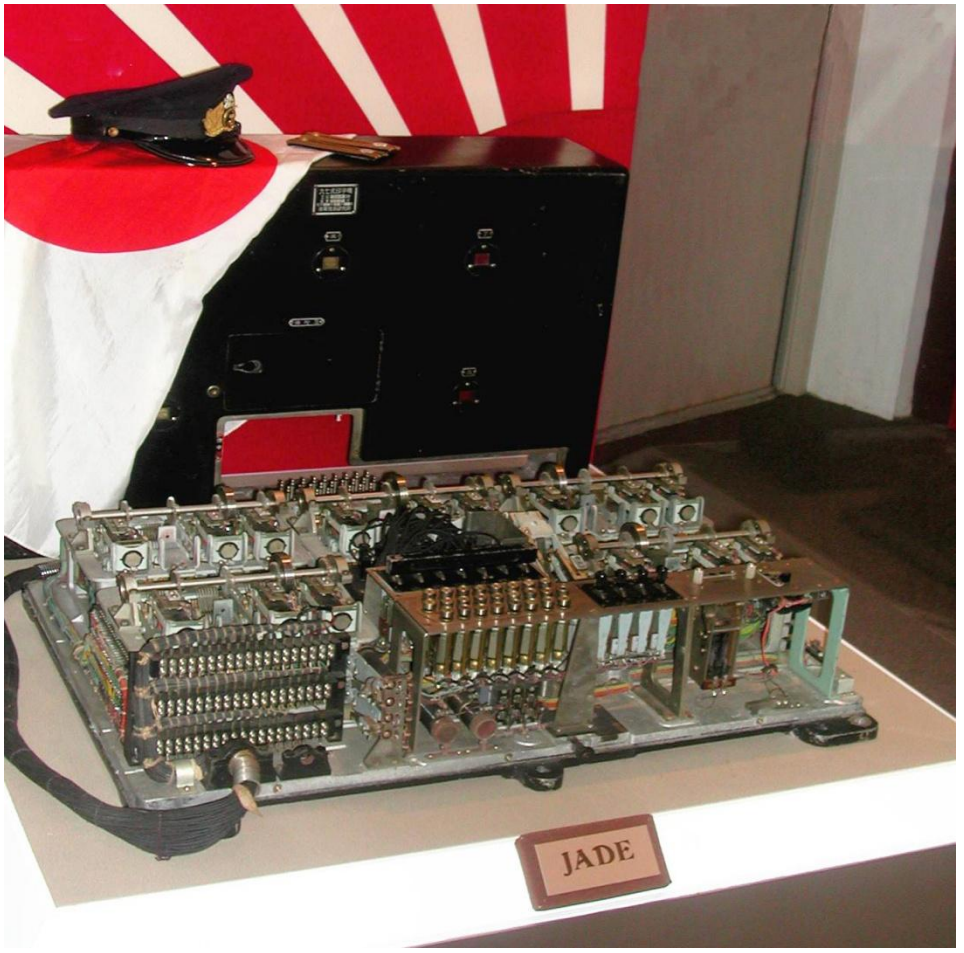




ECM Mark II rotor cage removed from the machine.

Japanese family of machines using telephone selector



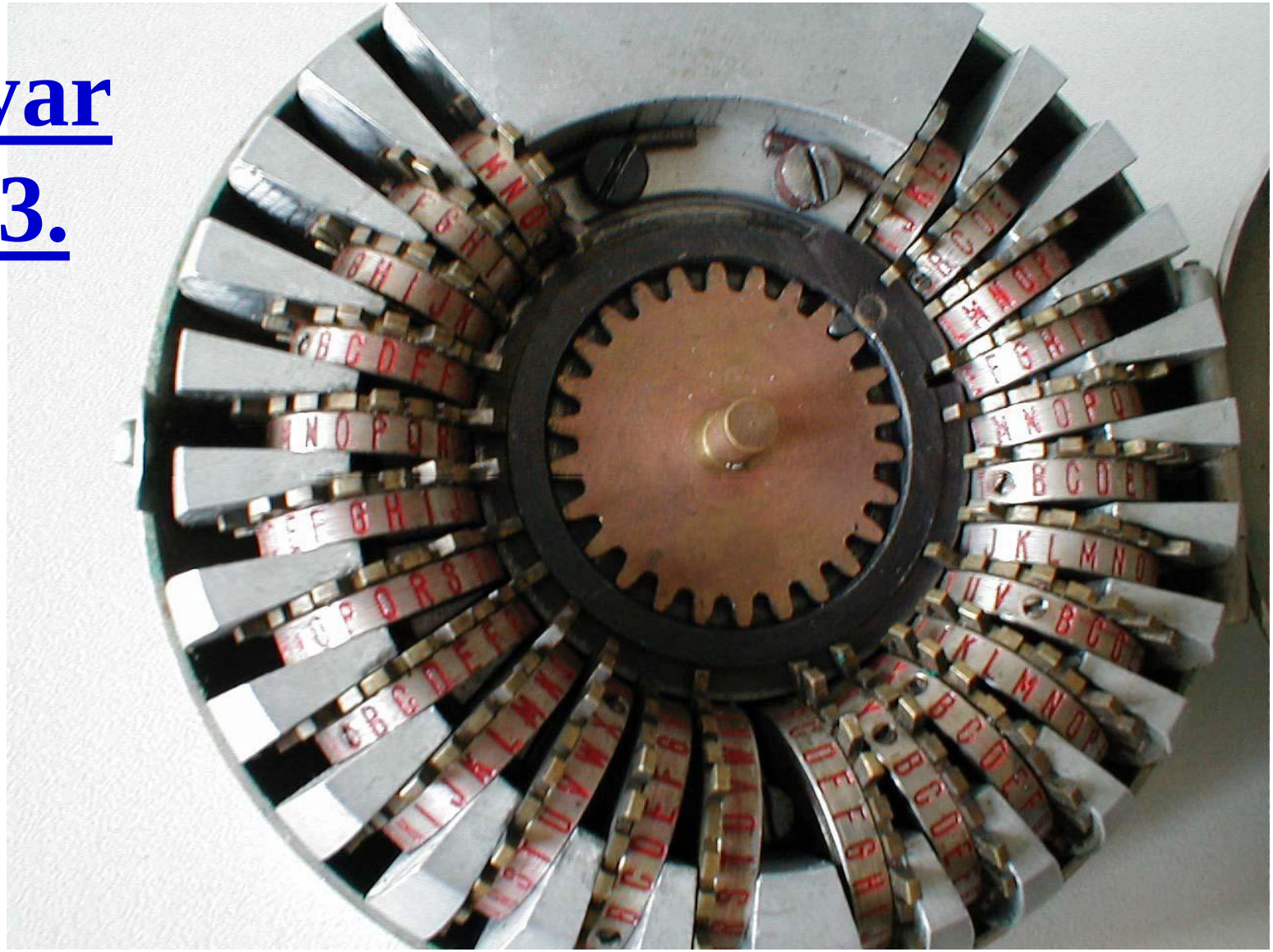


Magyar Dió 1.

Magyar köztársaaság Információs Hivatal

Magyar Dió 2.

Magyar Dió 3.



Great Seal of the United States (replica)

- On August 4, 1945, Soviet school children gave a carving of the Great Seal of the United States to U.S. Ambassador Averell Harriman.
- The microphone hidden inside was passive and only activated when the Soviets wanted it to be
- The Soviets were able to eavesdrop on the U.S. ambassador's conversations for six years.

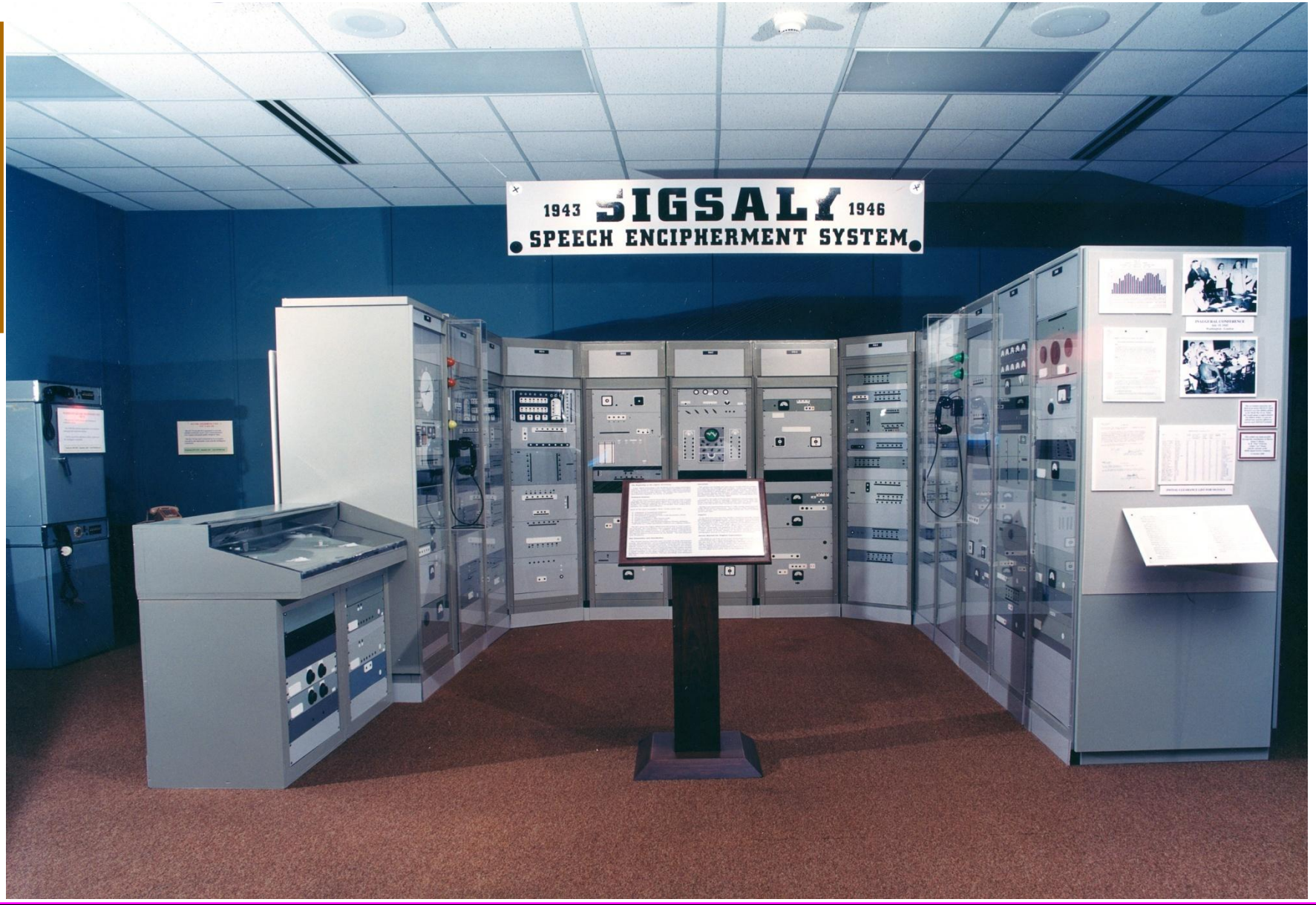
GRAB II (Galactic Radiation And Background) Satellite

- The second Signals Intelligence satellite to be launched by the United States.
- Launch of the GRAB II satellite: June 29, 1961

NSA

National Security Agency

SIGNALY



SIGSALY

- The **first secure voice encryption system** for telephones.
- Invented and built by Bell Telephone Laboratories in **1943**.
- It had several technological "firsts" **including pulse code modulation** for speech transmission, **multilevel frequency shift keying**, and **bandwidth compression.**
- The exhibit is a mock-up of one-third of the entire system, which weighed **55 tons** and consisted of forty racks of equipment.
- It took **thirteen people** to operate and required **fifteen minutes** to set up a phone call.
- The first two units were installed in the Pentagon in Washington, DC and in the basement of a popular London department store.
  (It was too large to fit in Churchill's war chambers.)
- During and after the war, units were installed worldwide totaling twelve locations for secure telephonic communications.

FIELD MANUAL NO 34-40-2

HEADQUARTERS - DEPARTMENT OF THE ARMY

Washington, DC, 13 September 1990

FOR OFFICIAL USE ONLY

BASIC CRYPTANALYSIS

TABLE OF CONTENTS

*This publication supersedes TM 32-220, 20 August 1970.

FOR OFFICIAL USE ONLY

George Orwell: 1984; (ford. Szíjgyártó László)

Winston elfordított egy kapcsolót, mire a hang valamivel halkabb lett, a szavakat azonban még mindig tisztán lehetett érteni. **A készüléket (teleképnek nevezték) le lehetett halkítani, de teljesen kikapcsolni sohasem lehetett. …**

A telekép egyszerre volt vevő- és adókészülék. Akármilyen hangot idézett elő Winston - az egészen halk suttogáson kívül -, a készülék felvette. Sőt: ameddig a fémlap látómezején belül tartózkodott, **nemcsak hallhatták, hanem láthatták** is….

Bizonytalan volt, hogy a **Gondolatrendőrség** milyen gyakran és milyen rendszer szerint kapcsolódik be egy-egy magán-teleképkészülékbe. Még az is elképzelhető volt, hogy mindenkit állandóan figyelnek. …

Az embernek abban a tudatban kellett élnie - s abban a tudatban is élt, ösztönné vált megszokásból -, hogy **minden hangját hallják, s kivéve, ha sötét van, minden mozdulatát megfigyelik.**

ECHELON = HARCLÉPCSŐ

- **"Spies like US":**

  London, Daily Telegraph, December 16, 1997

- quoted an unofficial **European Union report** on existence of ECHELON used to check European telecommunication

- ***"Within Europe all email, telephone, and fax communications are routinely intercepted by the United States National Security Agency transferring all target information from the European mainland via the strategic hub of London then by satellite to Fort Meade in Maryland via the crucial hub at Menwith Hill in the North York moors in the UK."***

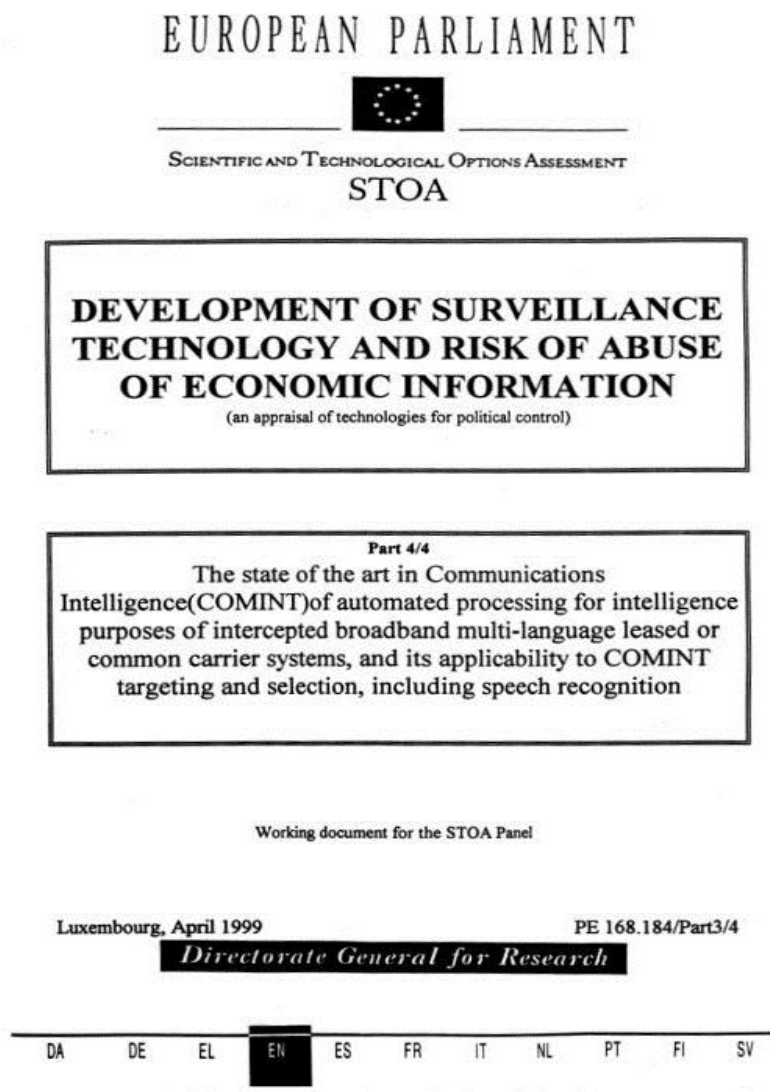
- Related issues:
  - civil liberties rights vs. national and public security (Big Brother)
  - technological / industrial / economical / military spying
  - organized crime:

    ➔ main issue: content or network ot communication (prepaid GSM telephones)

After: S.Katzenbeisser, F.A.P. Petitcolas: INFORMATION HIDING, techniques for steganography and digital watermarking; Artech House

European Parliament: STOA report (Scientific and Technical Options Assessment)

Development of Surveillance Technology and Risk of Abuse of Economic Information April 1999



EUROPEAN PARLIAMENT

SCIENTIFIC AND TECHNOLOGICAL OPTIONS ASSESSMENT
STOA

DEVELOPMENT OF SURVEILLANCE TECHNOLOGY AND RISK OF ABUSE OF ECONOMIC INFORMATION
(an appraisal of technologies for political control)

Part 4/4
The state of the art in Communications Intelligence(COMINT)of automated processing for intelligence purposes of intercepted broadband multi-language leased or common carrier systems, and its applicability to COMINT targeting and selection, including speech recognition

Working document for the STOA Panel

Luxembourg, April 1999 PE 168.184/Part3/4

Directorate General for Research

DA DE EL EN ES FR IT NL PT FI SV

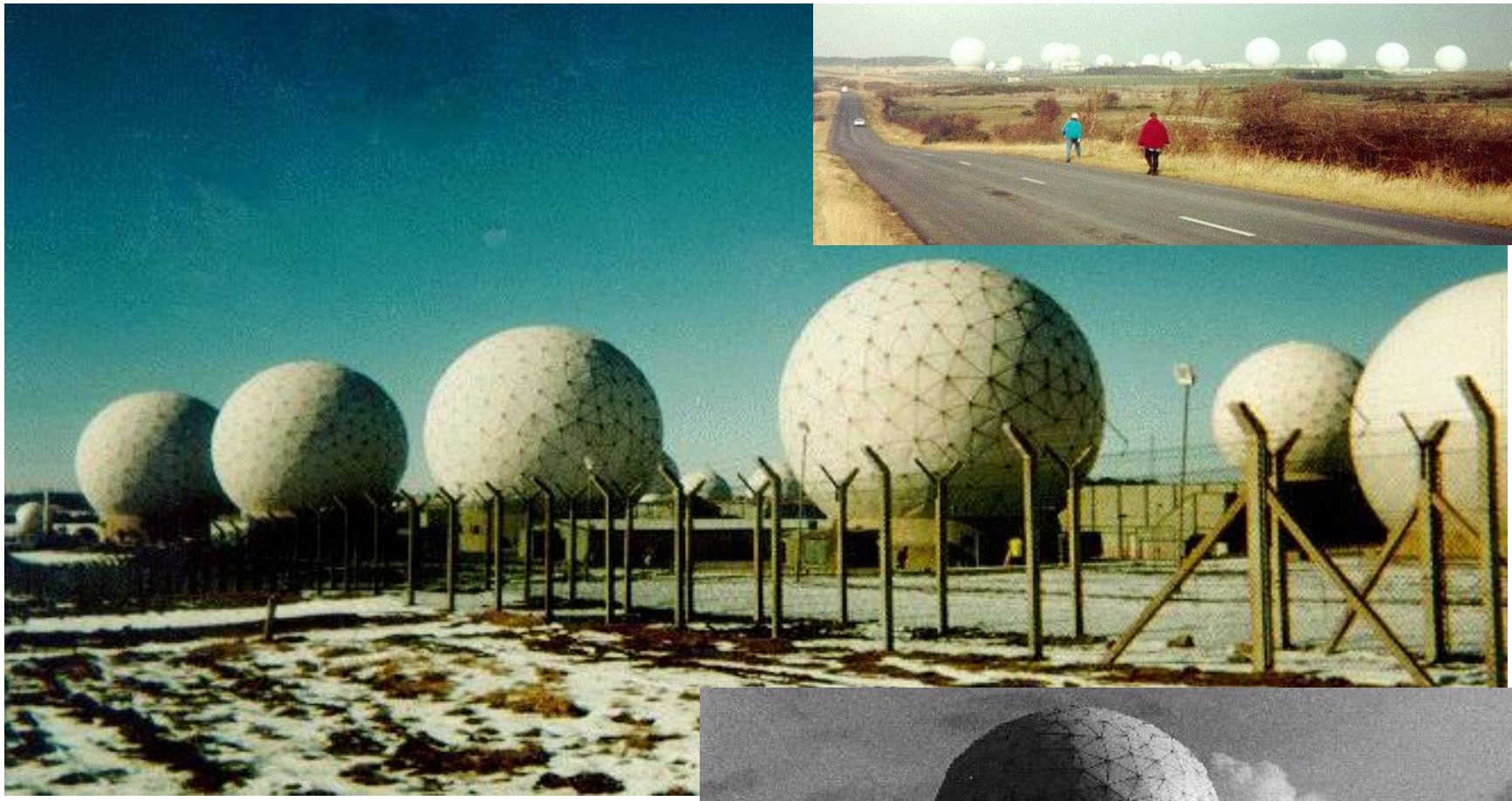
STOA_cover page

Globales elektronisches Aufklärungssystem

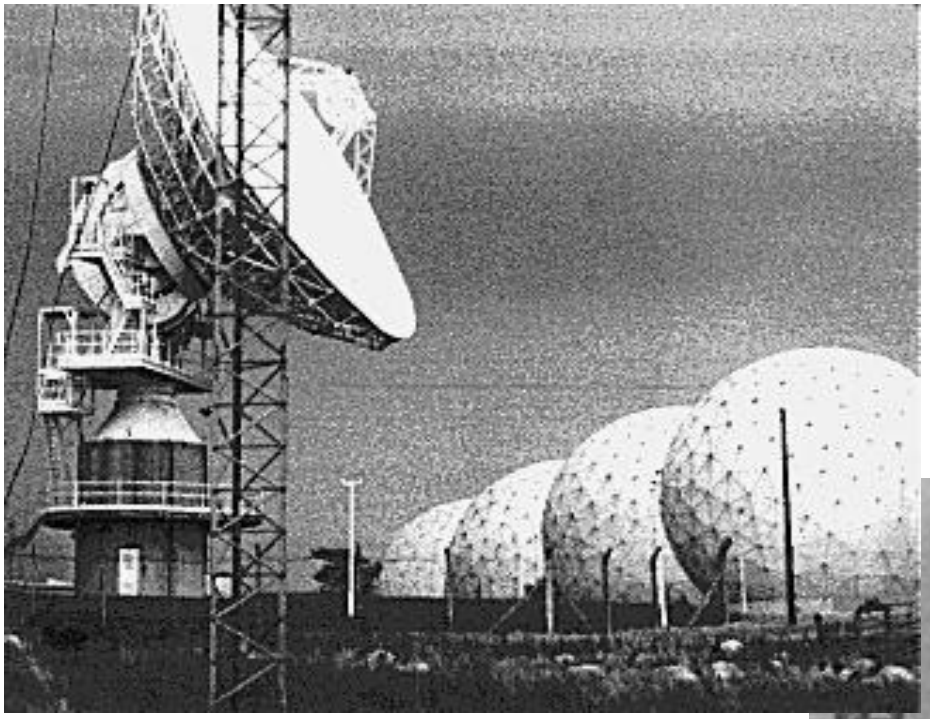
Echelon

Echelon hört ungefiltert den gesamten eMail-, Telefon-, Fax- und Telexverkehr ab, der weltweit über Satelliten weitergeleitet wird.

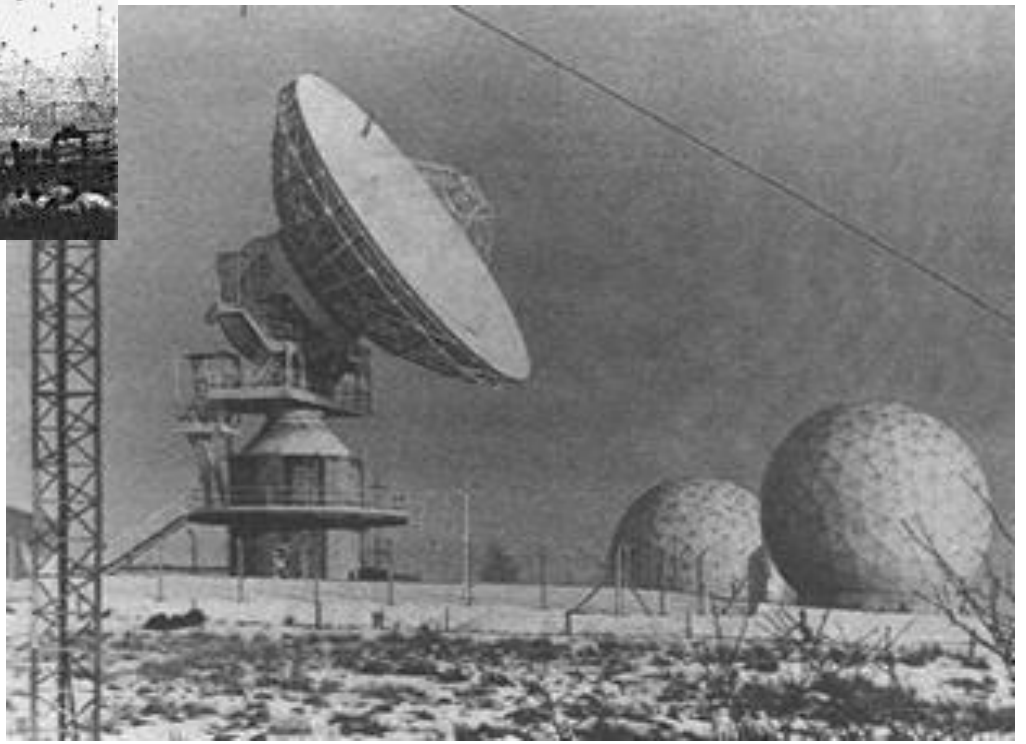
Grafik: Landesamt für Verfassungsschutz Baden-Württemberg



[Menwith Hill Station, UK 54.0162 N;1.6826 W)]

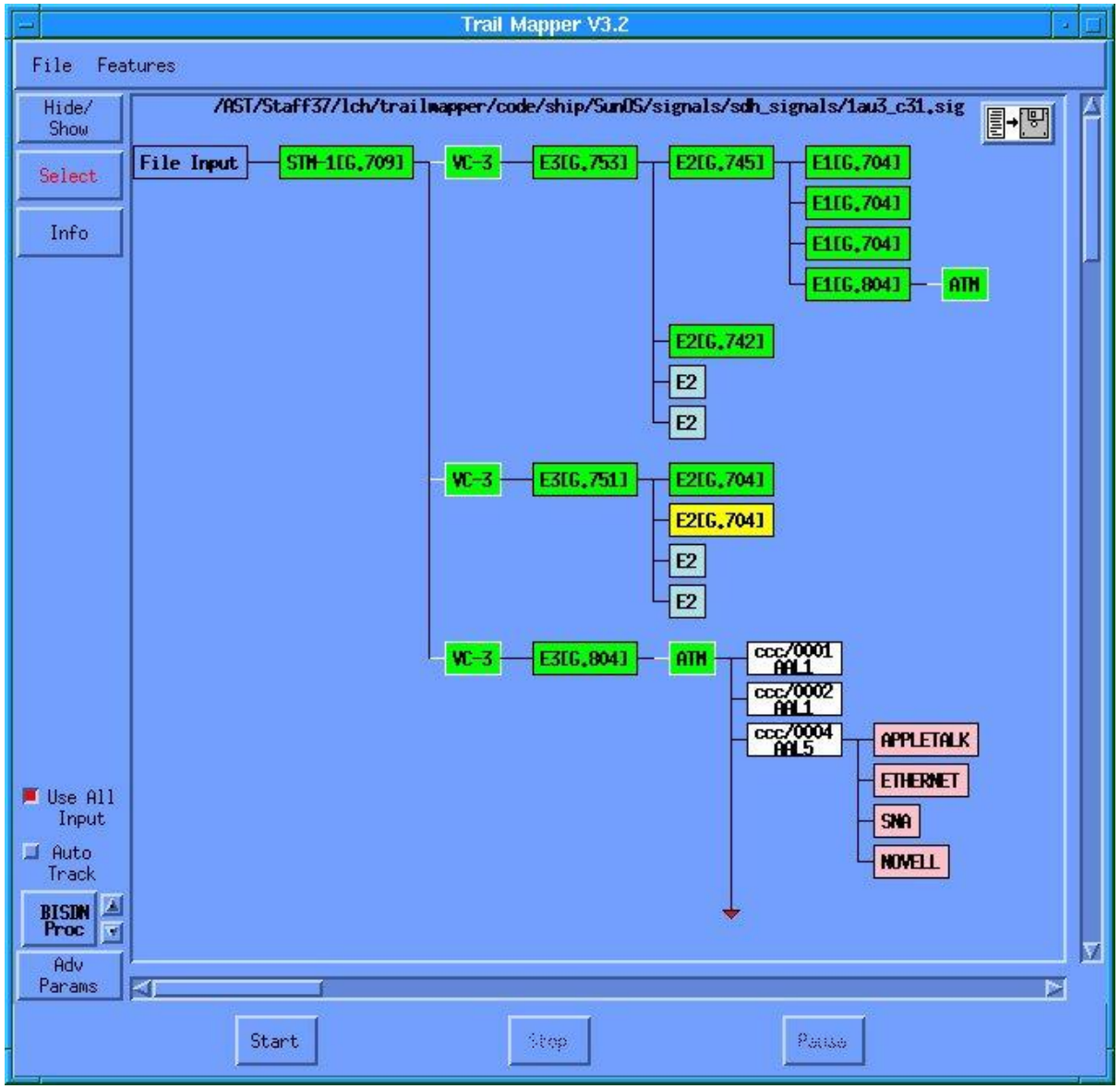


Menwith Hill Station, UK (54.0162 N; 1.6826 W)



Menwith Hill Station, UK (54.0162 N; 1.6826 W)

Overhead View of
Bad Aibling Station
Operations
(Photo courtesy of Jimmy Padgett)

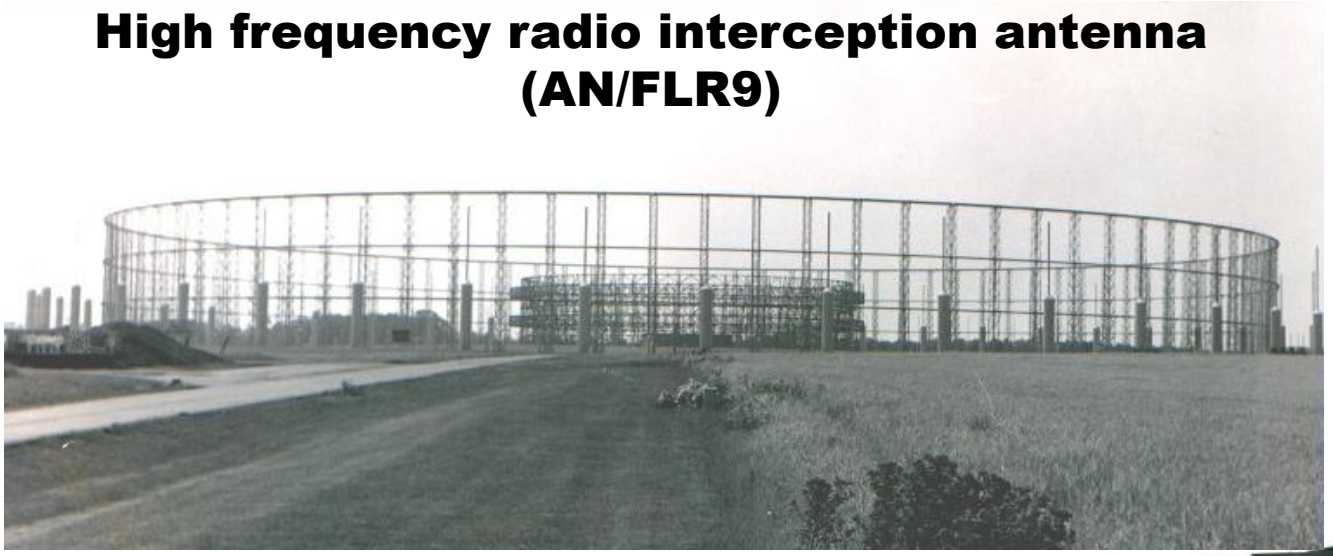


NSA "Trailmapper" software

- showing automatic detection of **private networks** inside intercepted high capacity **STM-1** digital communications system
- Since 1990, almost all communications have been digital, and are providing ever higher capacity. The highest capacity systems in general use for the Internet, called **STM-1** or **OC-3**, operates at a data rate of 155Mbs

INTERCEPTION CAPABILITIES 2000: CHICKSANDS

High frequency radio interception antenna (AN/FLR9)



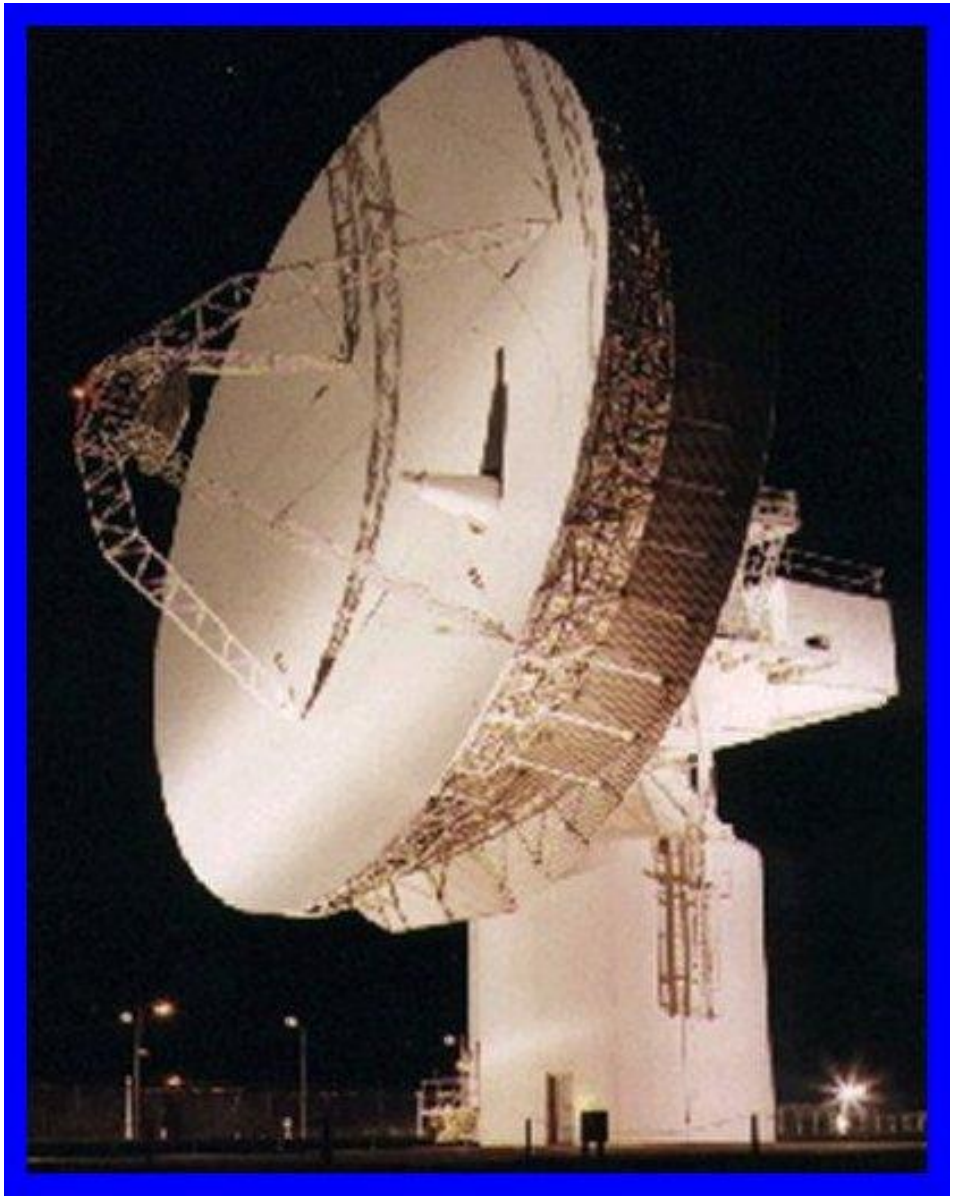
Report to the Director General for Research of the European Parliament

- **STOA: Scientific and Technical Options Assessment programme office**
  - on the development of surveillance technology and risk of abuse of economic information**.**
- This study considers the state of the art in Communications intelligence (**Comint**) of automated processing for intelligence purposes of intercepted broadband multi-language leased or common carrier systems, and its applicability to Comint targeting and selection, including **speech recognition** .

IC2000 Satellite ground terminal at Etam, West Virginia

connecting Europe and the US via Intelsat IV

IC2000: British Comint agency GCHQ

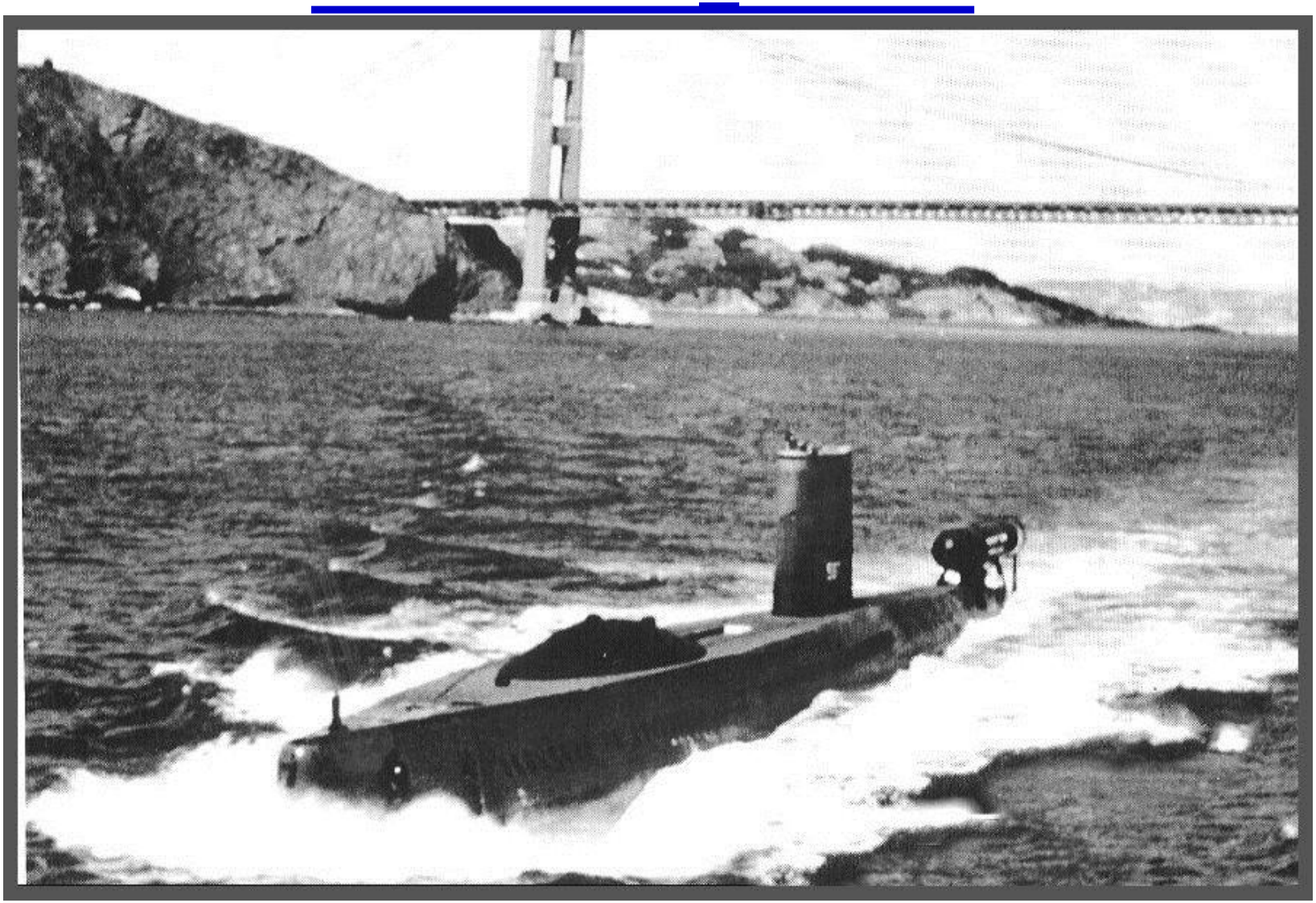


- GCHQ
  - Government Communications Headquarters;
  - the Sigint agency of the United Kingdom
- constructed an identical "shadow" station in 1972
  - to intercept Intelsat messages for UKUSA

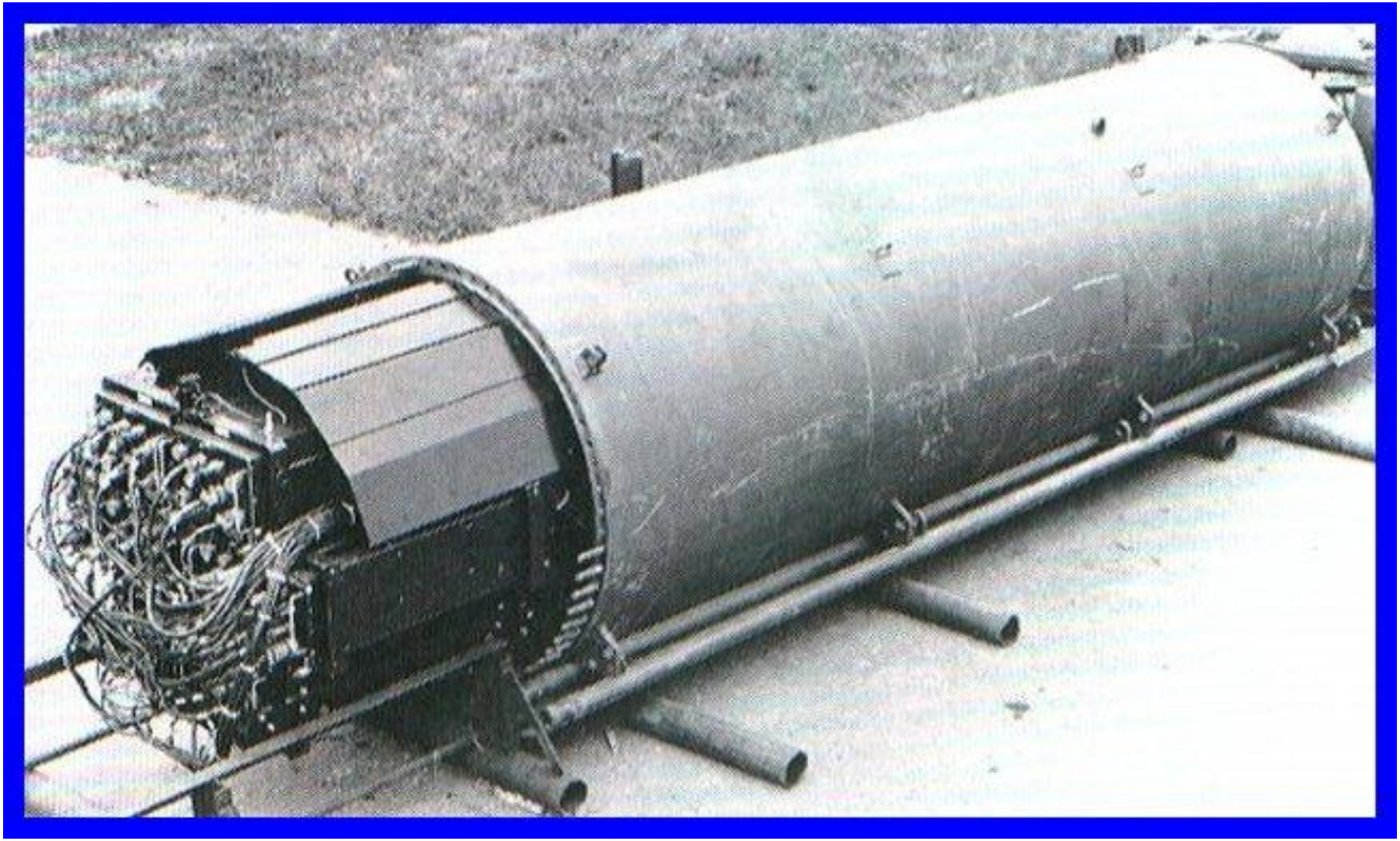
IC2000: Submarine cable interception

- Submarine cables playd a dominant role in international telecommunications, since
  - in contrast to the limited bandwidth available for space systems - optical media offer seemingly unlimited capacity.
  - Safe where cables terminate in countries where telecommunications operators provide Comint access (such as the UK and the US),
  - submarine cables appear intrinsically secure because of the nature of the ocean environment.
- In **October 1971**, this security was shown not to exist.
  - A US submarine, **Halibut**, visited the **Sea of Okhotsk** off the eastern **USSR** and recorded communications passing on a military cable to the **Khamchatka** Peninsula.
  - Halibut was equipped with a deep diving chamber, fully in view on the submarine's stern.
  - The chamber was described by the US Navy as a "deep submergence rescue vehicle".
  - The truth was that the "rescue vehicle" was welded immovably to the submarine.
  - Once submerged, deep-sea divers exited the submarine and wrapped tapping coils around the cable.
  - Having proven the principle, USS Halibut returned in **1972** and laid a high capacity recording pod next to the cable.
  - The technique involved no physical damage and was unlikely to have been readily detectable.

IC2000: uss_halibut

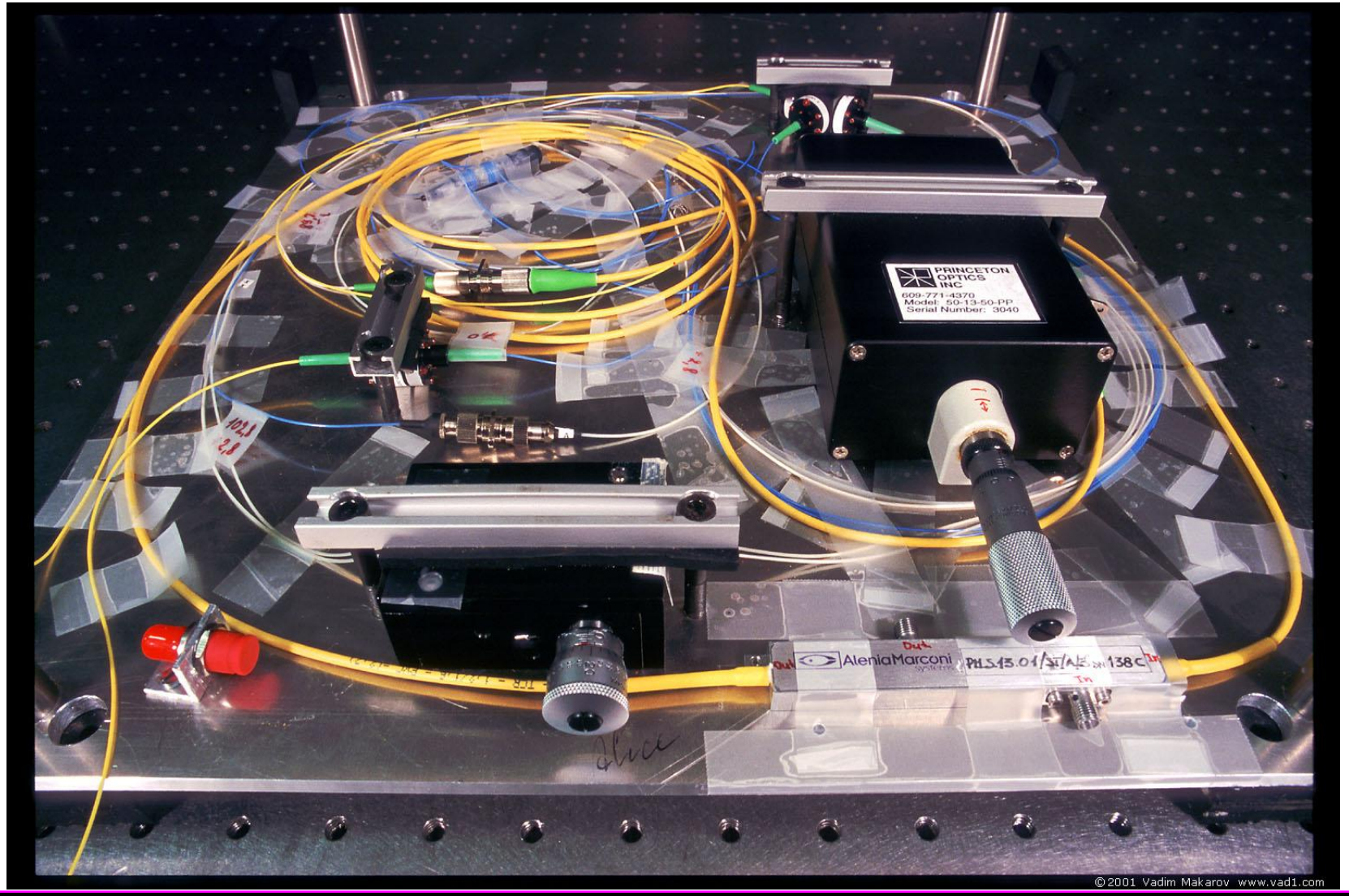


IC2000: Cable tapping pod laid by US submarine off Khamchatka



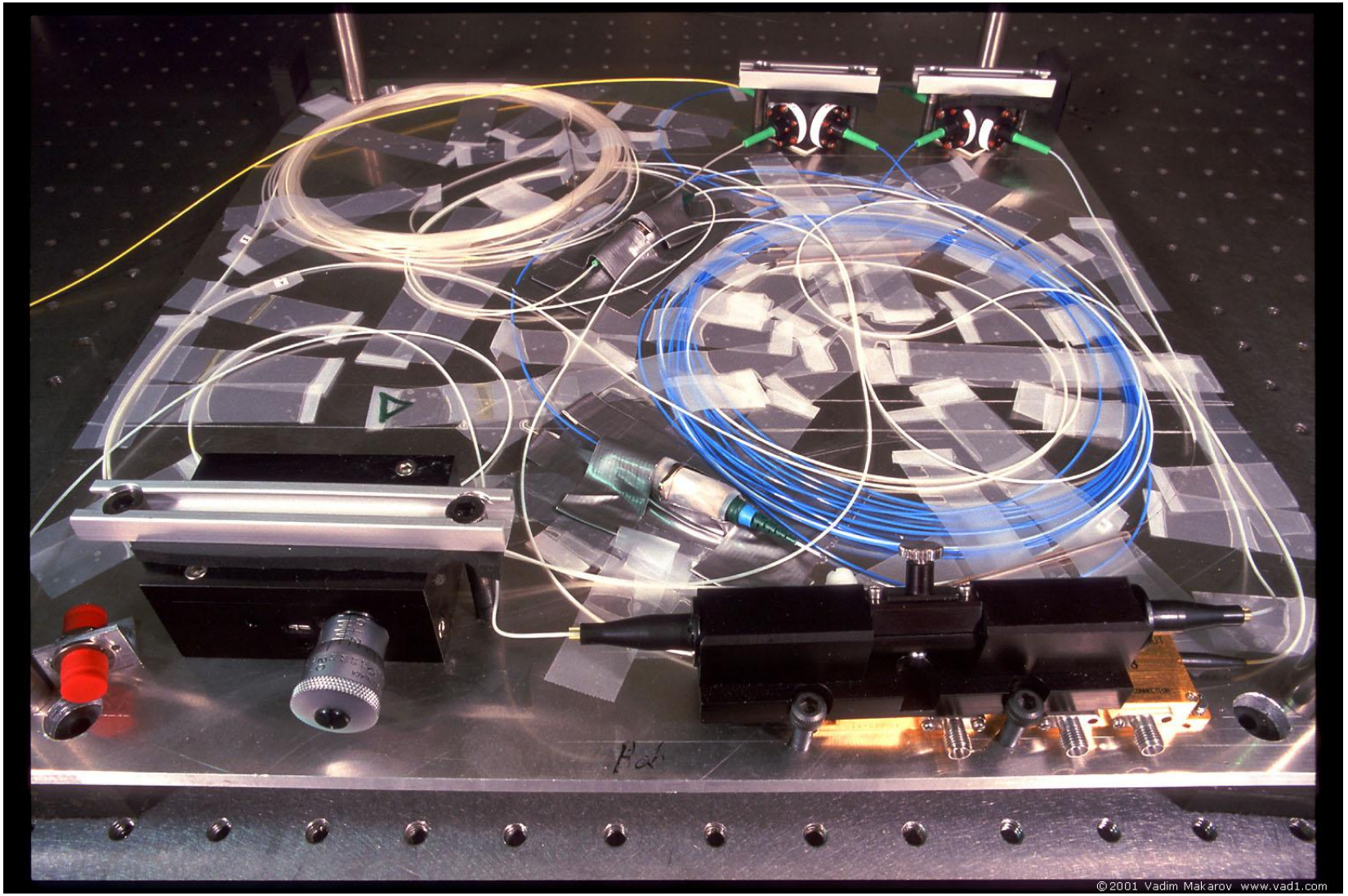
Quantum Cryptography in Norway ; Quantum cryptography system.

- **Alice's optical setup (uncovered, no thermoisolation installed)**



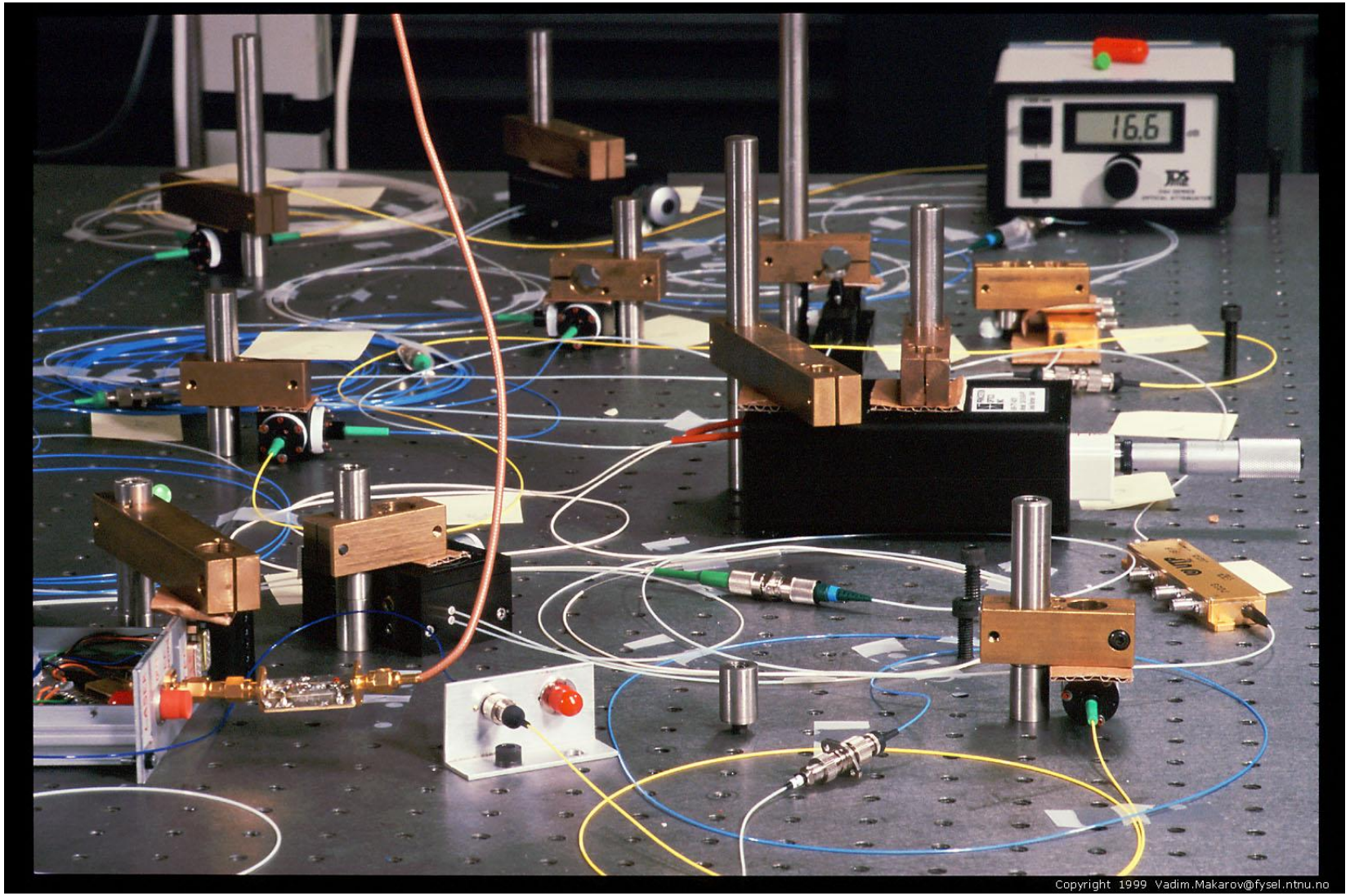
Quantum Cryptography in Norway ; Quantum cryptography system.

- Bob's optical setup (uncovered, no thermoisolation installed)



Quantum Cryptography in Norway ; Quantum cryptography system.

- Quantum key distribution setup in testing stage - laying on optical table



Quantum Cryptography in Norway ; Quantum cryptography system.

- Researcher tunes up eavesdropper's (Eve's) setup

KRIPTOGRÁFIAI ALGORITMUSOK és PROTOKOLLOK ÁTTEKINTÉS

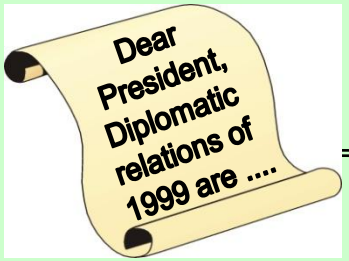
CRYPTOGRAPHIC ALGORITHMS and PROTOCOLS OVERVIEW

KRYPTOGRAPHISCHE ALGORITHMEN und PROTOKOLLEN ÜBERBLICK

SZIMMETRIKUS / TITKOS KULCSÚ REJTJELEZÉS

KÜLDŐ: A
Alice

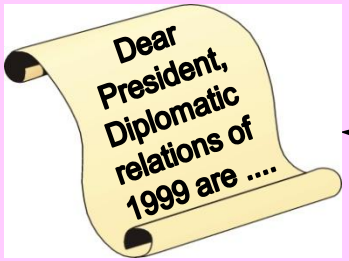
NYILT SZÖVEG



REJT-JELZÉS E_K

REJTETT SZÖVEG

NYILVÁNOS, NEM BIZTON-SÁGOS CSATORNA



MEG-OLDÁS D_K

TITKOS BIZTON-SÁGOS CSATORNA

KULCS CSERE

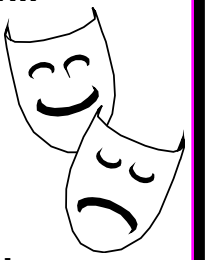
KAPCSOLAT KULCS

FOGADÓ: B
Bob

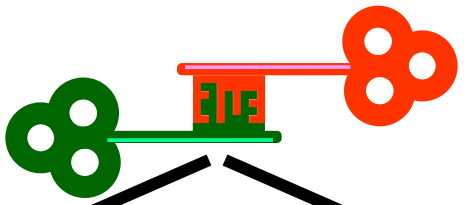
- Kis kulcs titkos átküldése a nagy üzenet helyett
- Gyors.
- Kell egy biztonságos csatorna a kulcscseréhez.
- Nehézkes, korábban egymást nem ismerő, nagy csoportok kommuniká-ciójára

ASZIMMETRIKUS / NYÍLVÁNOS KULCSÚ REJTJELEZÉS (PKC)

- Minden résztvevőnek van egy kulcspárja: egyik nyilvános, másik titkos.
- A nyilvános kulccsal rejtjelezett adatot, csak a titkos kulccsal lehet visszanyerni, megoldani.
- Lassú. Nagy méretű adatok rejtjelezésére nehézkes. Hibrid megoldások.
- A nem biztonságos nyilvános csatornát átalakija biztonságossá. Alkalmas kulcs cserére.
- Használhatóvá teszi a szimmetrikus kulcsú rejtjelezést nyilvános csatornán, nagy, egymást előzőleg nem ismerő csoportok számára is.
- Tekinthetjük a Kapcsolat Kulcs "**DIGITÁLIS BORÍTÉKJÁNAK"**



KUCSCSERÉRE HASZNÁLT NYILVÁNOS KULCSPÁR LÉTREHOZÁSA ÉS SZÉTOSZTÁS



AKTÍV MEGSZEMLYESÍTÉSI TÁMADÁS: nyilvános kulcs hamisítása. Annak hitelesnek kell lennie, azaz egy Megbízható Harmadik Fél (TTP) által tanúsítottnak.

KÜLDŐ: A

FOGADÓ NYILVÁNOS KULCSA, K_P^B

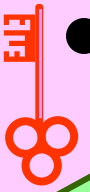
REJTJELZÉS

KAPCSOLATKULCS, SK

KAPCSOLATKULCS BIZTONSÁGOS CSERÉJE NYILVÁNOS CSATORNÁN

FOGADÓ: B

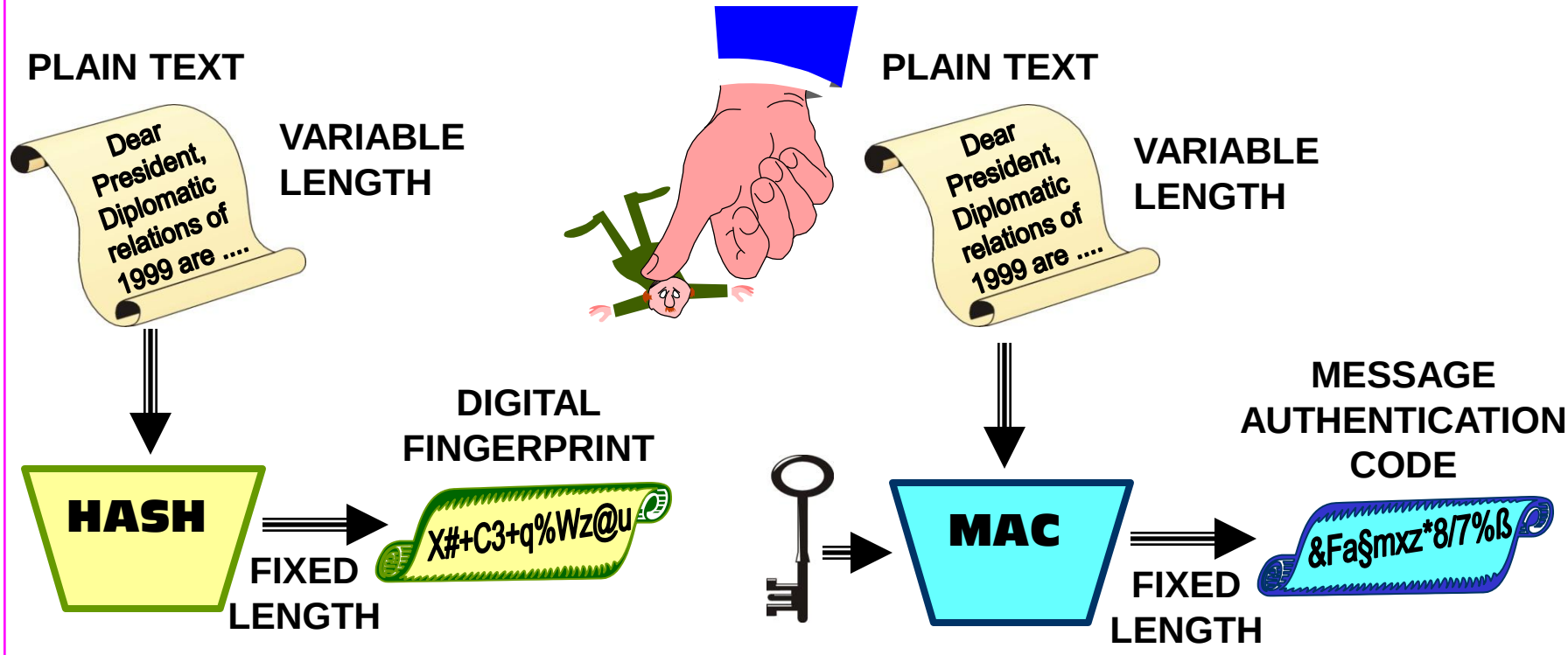
FOGADÓ TITKOS KULCSA, K_S^B



MEGOLDÁS

KAPCSOLATKULCS, SK

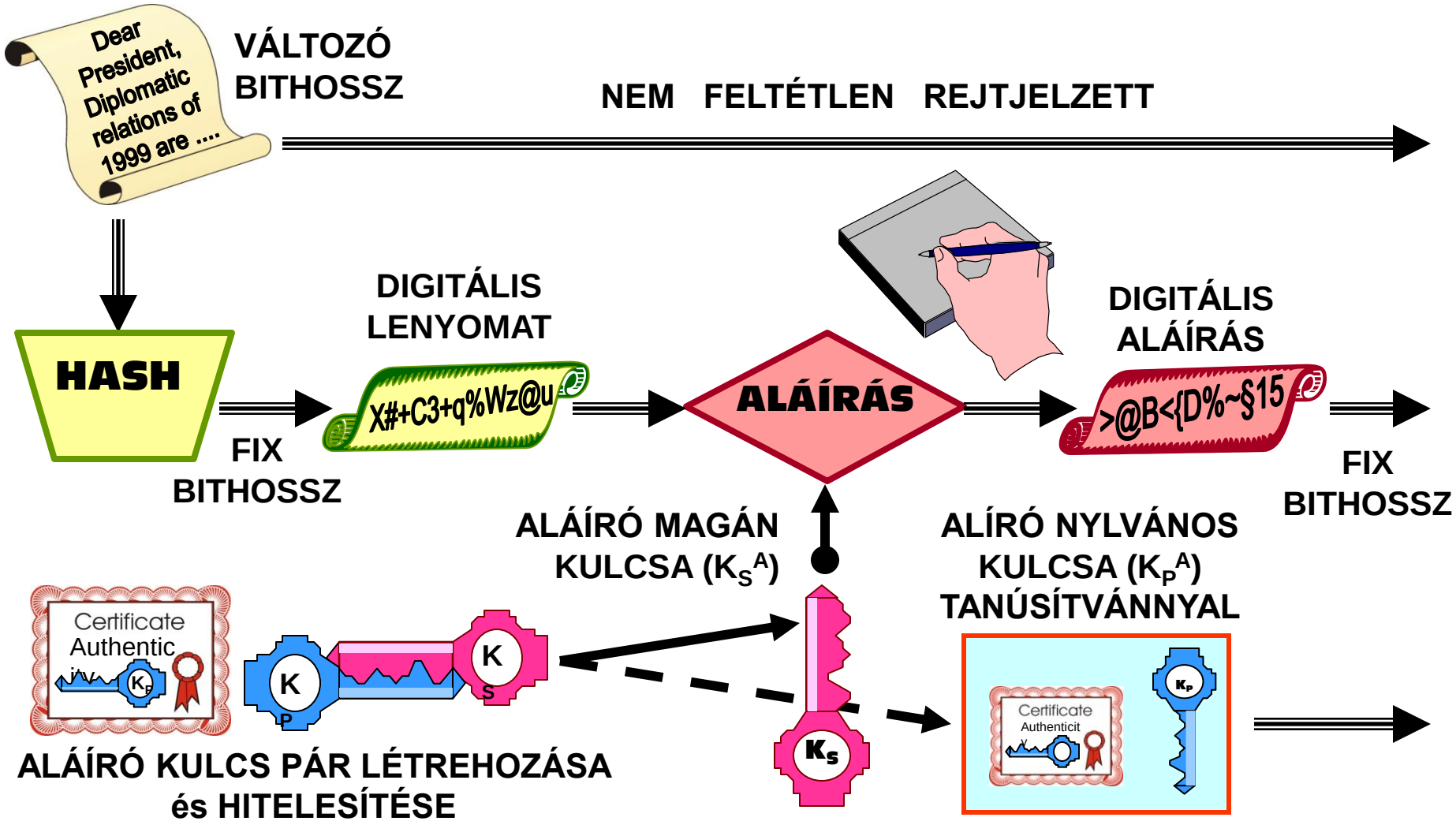
HASH FUNCTIONS and the MESSAGE AUTHENTICATION CODE (MAC)



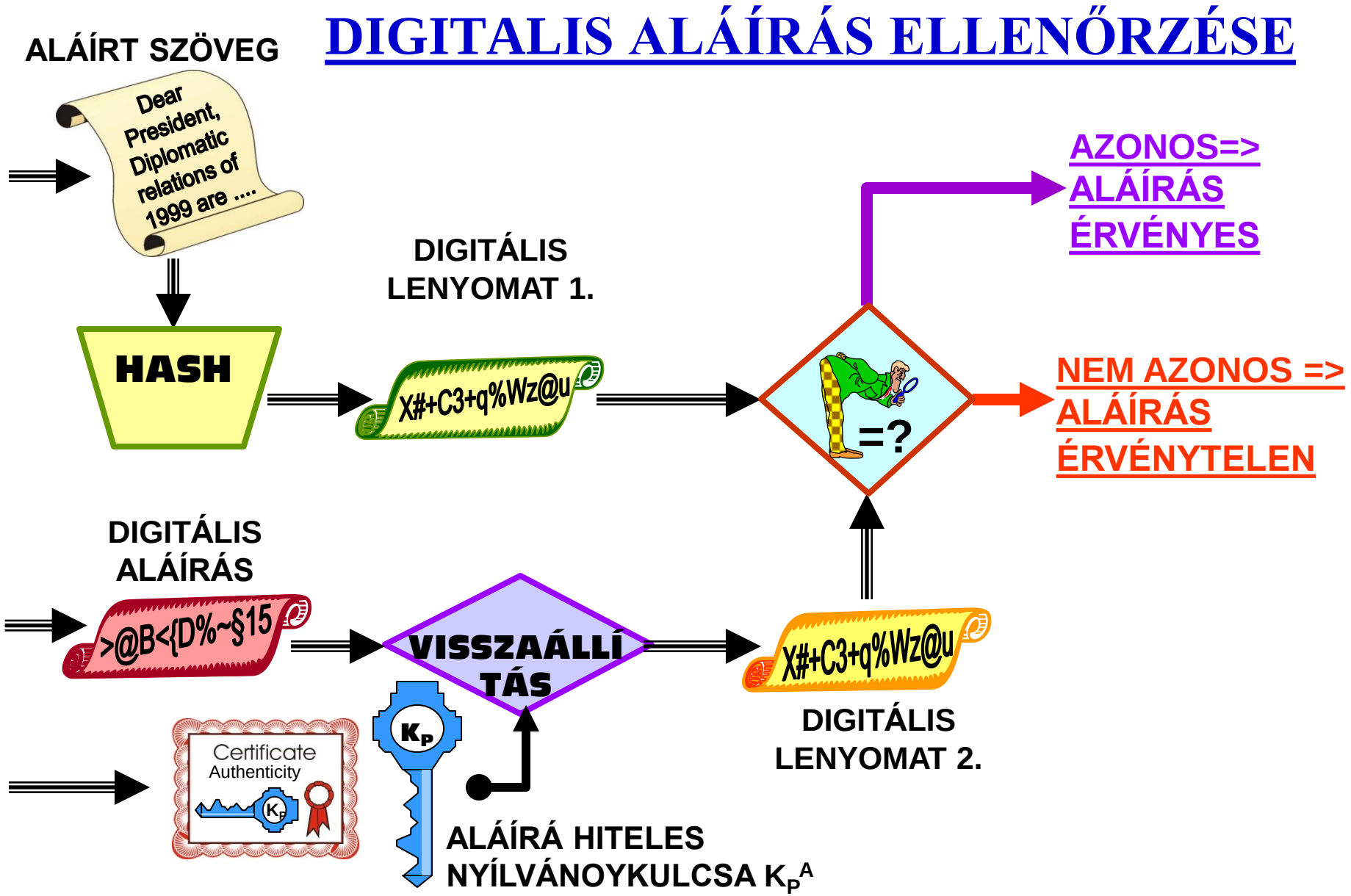
- They are standard one-way functions.
- Anyone can generate, alter and verify it.
- It is useful for digital signature.
- Many times it has to be protected.

- They are standard one-way functions with an added key, i.e. password.
- Only who knows the key (password) can generate, alter and verify it.
- It is useful for message authentication.

DIGITALIS ALÁÍRÁS LÉTREHOZÁSA



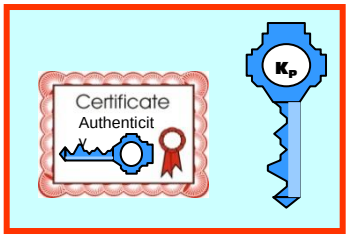
DIGITALIS ALÁÍRÁS ELLENŐRZÉSE



VAK ALÁÍRÁS

ALÁÍRANDÓ SZÖVEG

Dear President, Diplomatic relations of 1999 are ....



ALÁÍRÓ NYÍLVÁNOS KULCSA és TANÚSÍTVÁNYA (K_P^A)

HASH

X#+C3+q%Wz@u

DIGITÁLIS LENYOMAT

ELTAKARÁS

ELTAKARÓ KULCS

ELTAKART DOKUMENTUM / LENYOMAT

>@B<{D%~§15

KITAKART DIGITÁLIS ALÁÍRÁS

KITAKARÁS

KITAKARÓ KULCS

>@B<{D%~§15

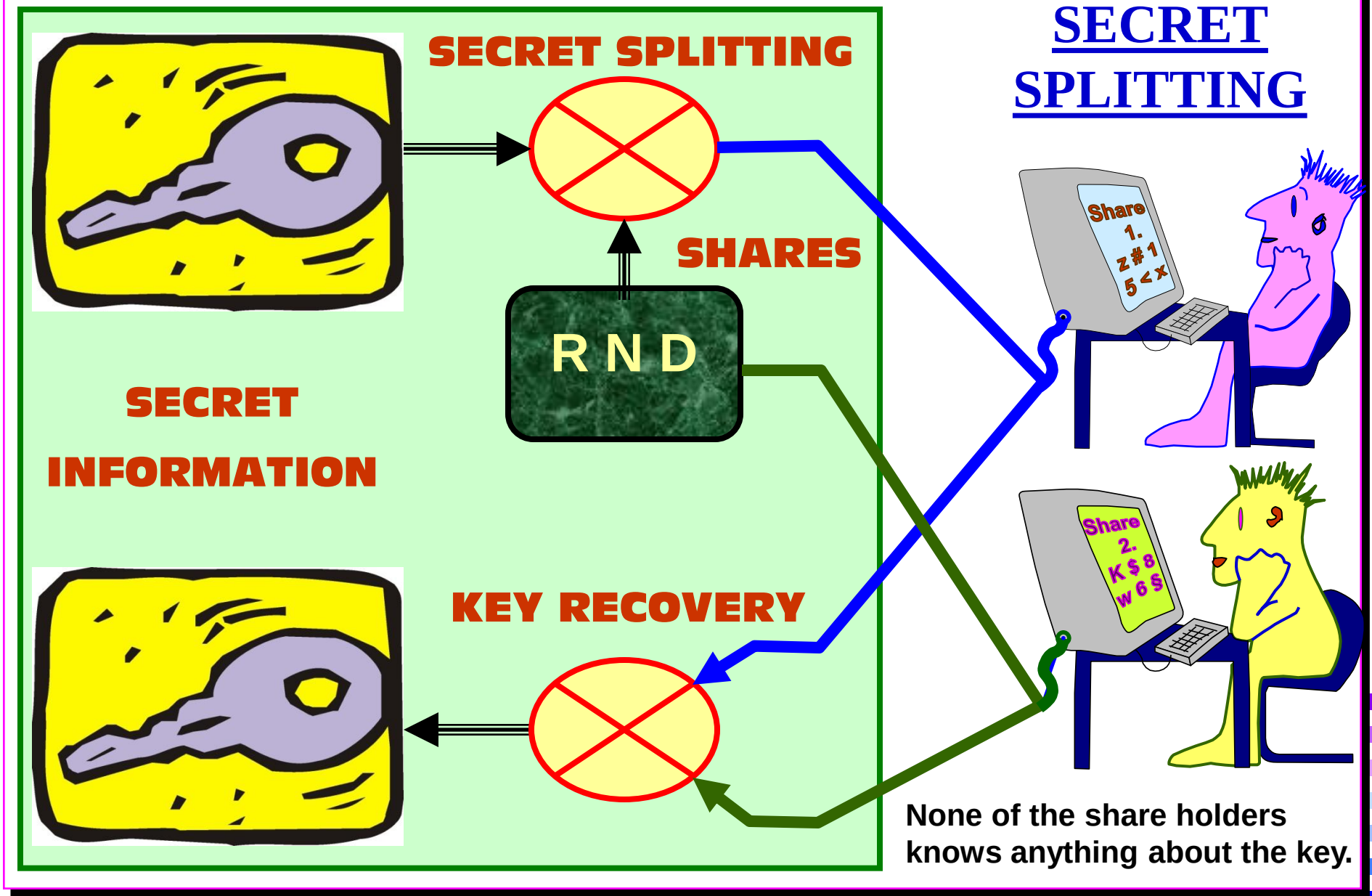
ELTAKART DIGITÁLIS ALÁÍRÁS

ALÁÍRÓ

ALÁÍRÁS

ALÁÍRÓ MAGÁN KULCSA (K_S^N)

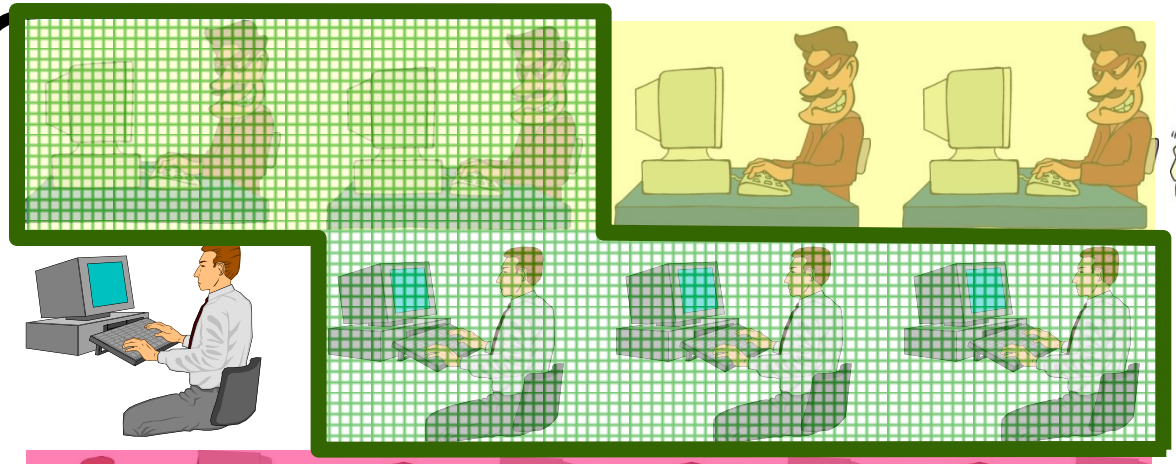
SECRET SPLITTING

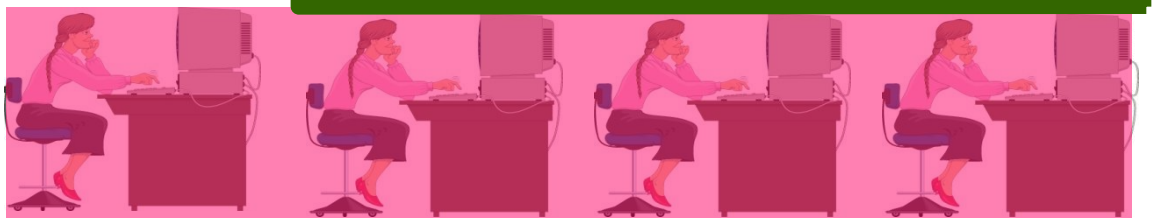


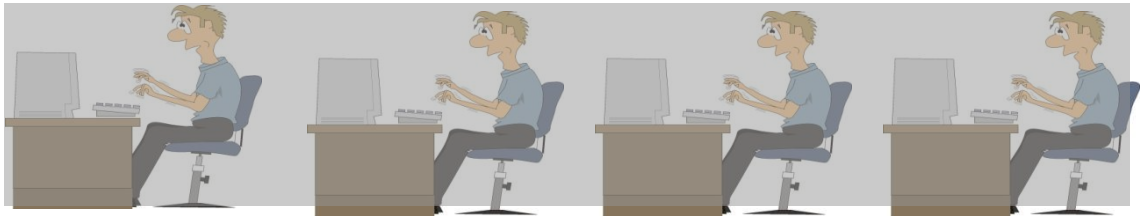
SECRET SHARING: 5 - OUT - OF - 20 SCHEME

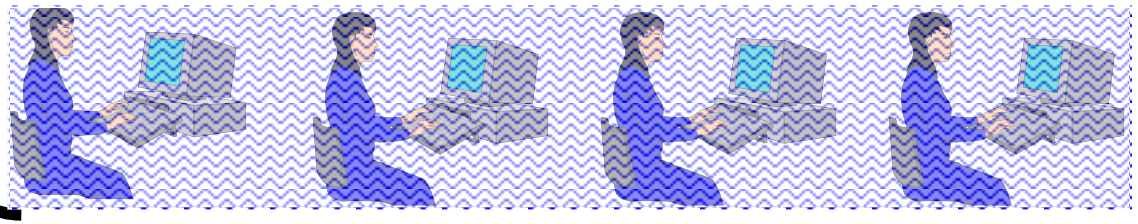
DEALER

SHADOWS









BRIBERS, HACKERS: 4 SHADOW ARE NOT ENOUGH

REGAIN the KEY from ANY 5 SHADOWS

FIRE, TECHNICAL BREAK-DOWN

SABOTAGE, EARTH-QUAKE, VIRUSES

FLOOD, WIND, HURRICANE

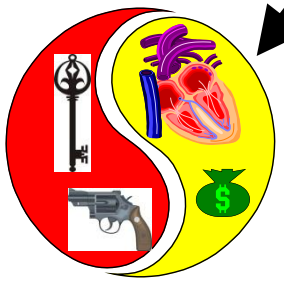
After:
S.Katzenbeisser;
F.A.P. Petitcolas:
INFORMATION
HIDING,
techniques for
steganography
and digital
watermarking;
Artech House

STEGANOGRAPHY

PRISONERS' PROBLEM

PRISONER
ALICE

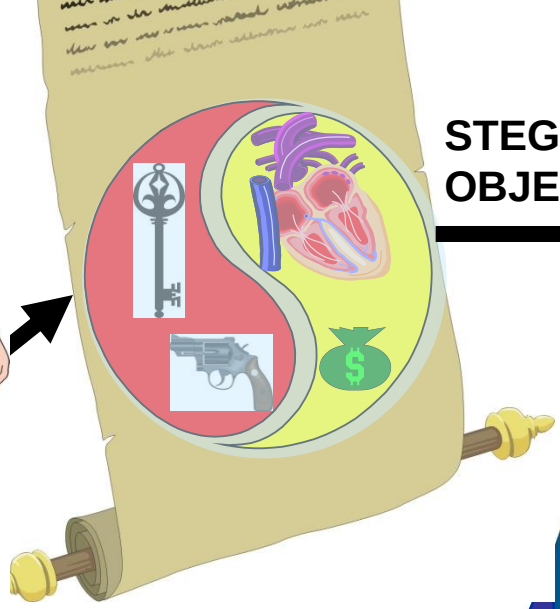
PRISONER
BOB



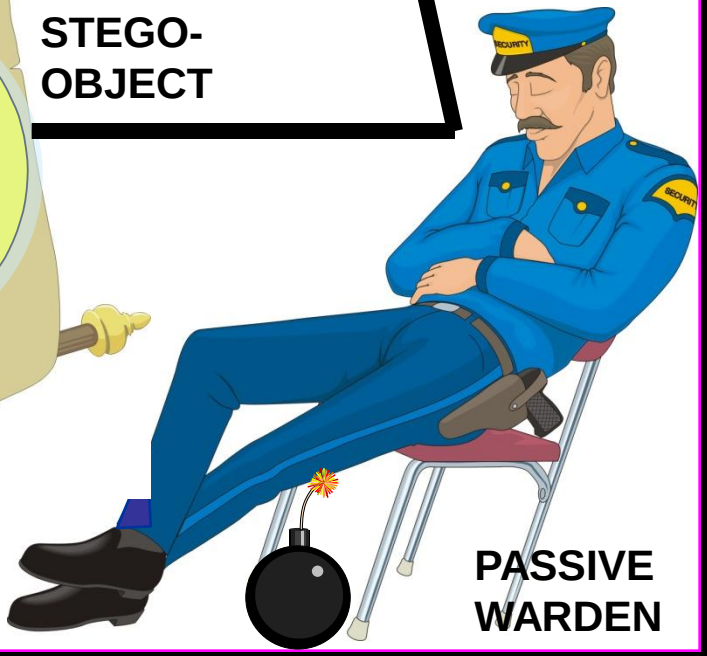
EMBEDDED
SECRET
MESSAGE

COVER

WENDY, the ACTIVE or
MALICIOUS WARDEN



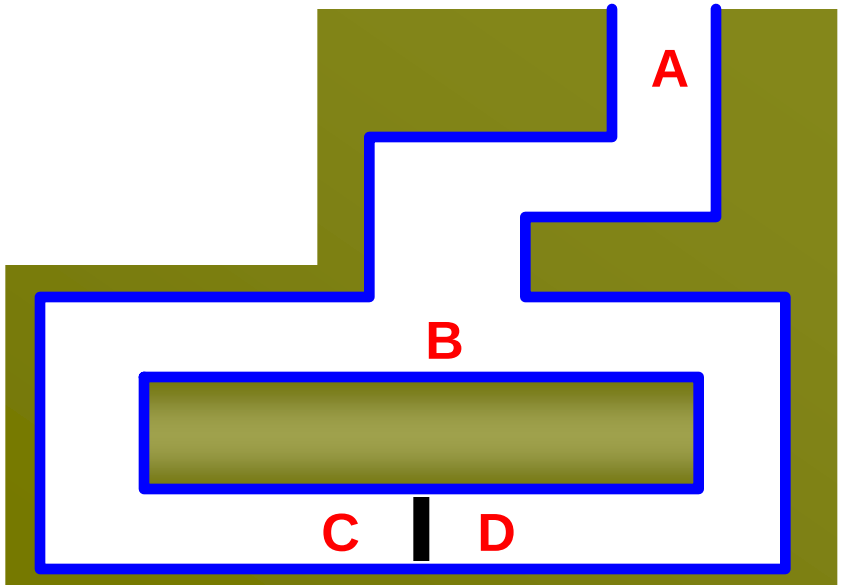
STEGO-
OBJECT



PASSIVE
WARDEN

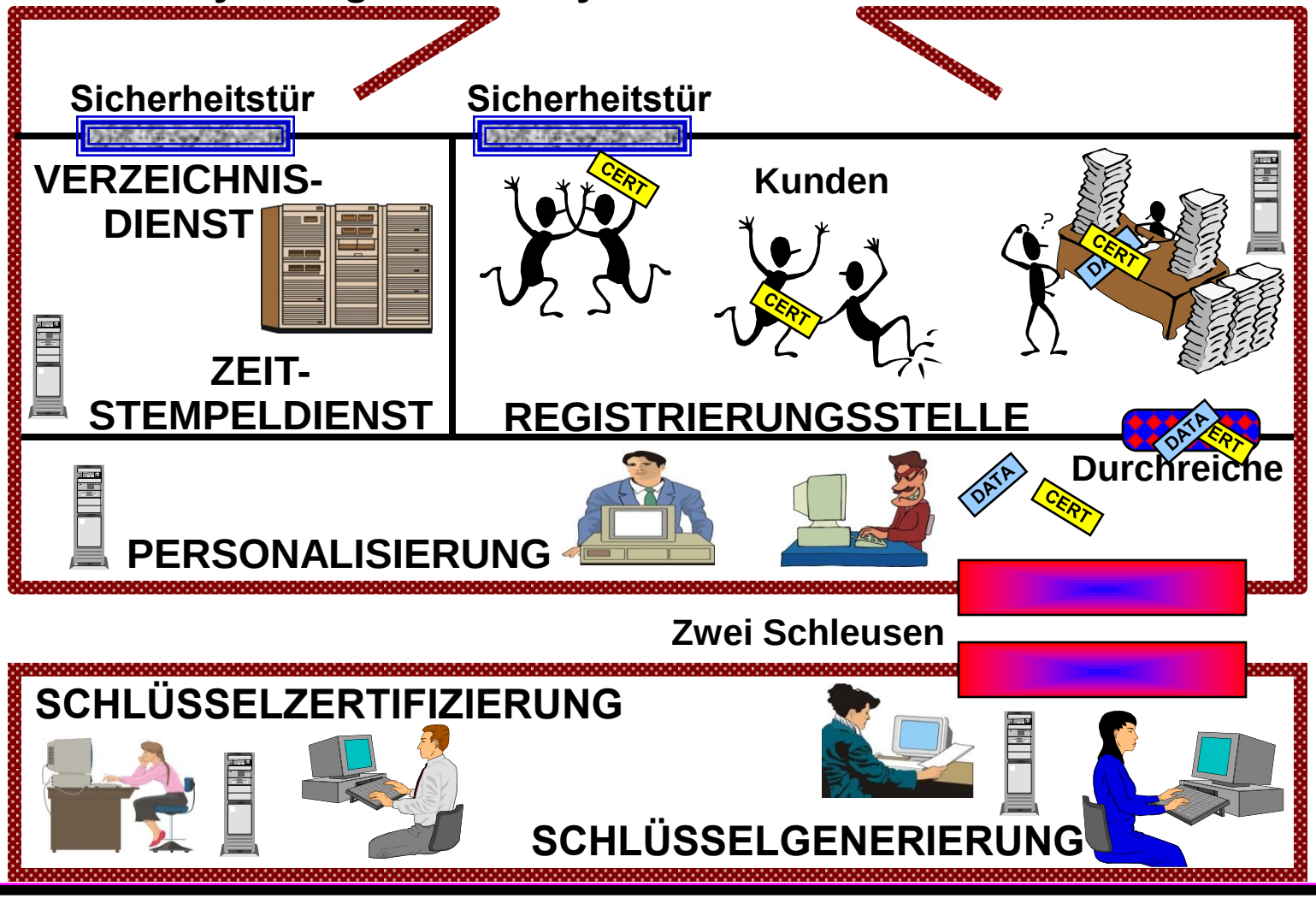
"NULLA ÉRTESÜLÉS" INTERAKTIV BIZONYÍTÁS: PÉLDA

- intuitív példa: **Ali Baba barlangja,** ahol **Aliz** a **bizonyító** és **Bob** a **vizsgáló:**
- **Aliz bizonyítani akarja Bobnak,** hogy ismeri a titkos varázsszót, amely kinyítja a C-D kaput **(állásfoglalás, commitment)**, de
- **nem akarja, hogy Bob megtudja a varázsszót.**
- **egy üzenetváltás-kőr lehet az alábbi:**
  - Aliz **állásfoglalása (commitment)**: el fog meni a C vagy D pontokhoz és a varázsszóval azt ki tudja nyitni;
  - Bob A-hoz megy és vár mig Aliz a C-hez vagy D-hez megy.
  - Bob ekkor a B ponthoz megy és üzeni (kiáltja), hogy azt akarja, hogy Aliz a jobb vagy a bal oldalról térjen vissza.
  - Bob addig ismétli azt az algoritmust ameddig akarja, ameddig biztos abban, hogy Aliz tudja vagy sem a varázsszót.
- Ha Aliz nem ismeri a varázsszót akkor 50% az esélye, hogy balról illetve jobbról térjen vissza; ha ismeri ez a valószínűségi eloszlás változik.
- Mindegy, hogy Bob meddig ismételgeti a fenti algoritmust, **semmit sem tud meg a varázsszóról.**
- Ha a varázsszót csak Aliz tudhatta, akkor Aliz **személyazonosságát** is hitelesítettük



CENTRAL MODEL of a CERTIFICATION AUTHORITY

- No branch offices
- The user's keys are generated by the CA

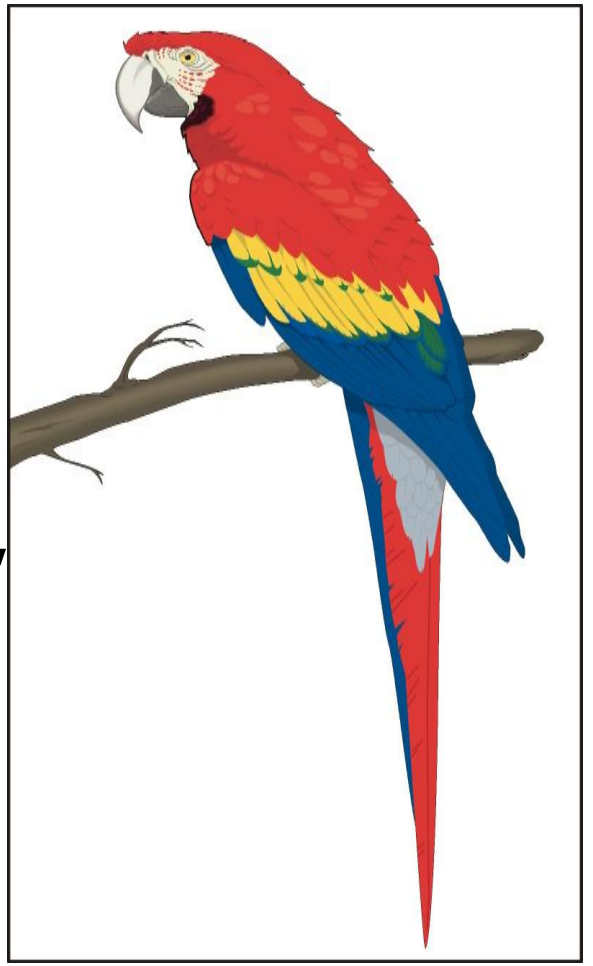


JELSZÓ BIZTONSÁG

Természetesen az én jelszavam is a kedvenc háziállatom neve.

A papagájom neve:

“Q47#XΦ>zöℜR5z×μ[§g_ä&Yß69ΘW 1$/^+?{℘!666Ψ%@ü>Σa5\[ä=3:j§±ΠŦ ■♦~”*



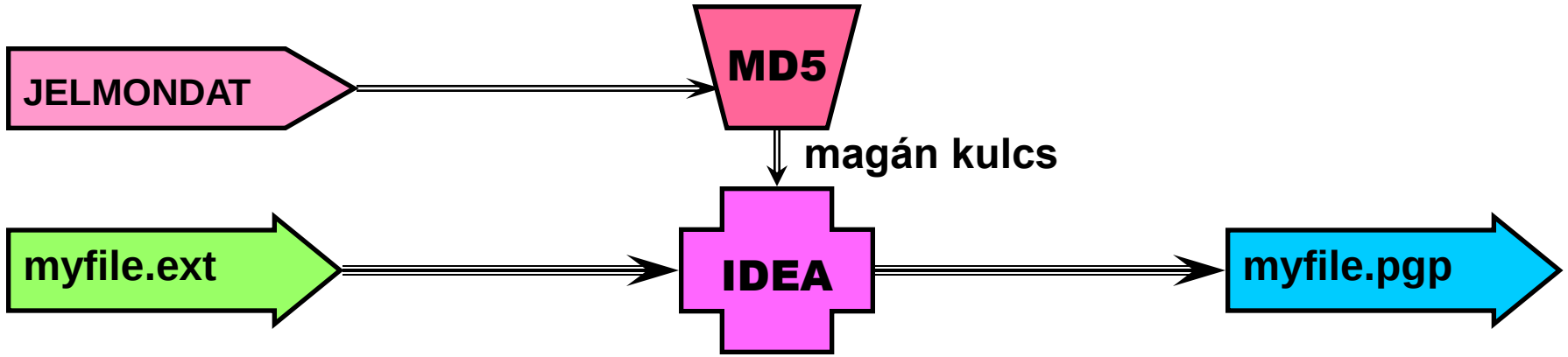
amit biztonsági okokból 3 havonta megváltoztatok.

Trevor Linton

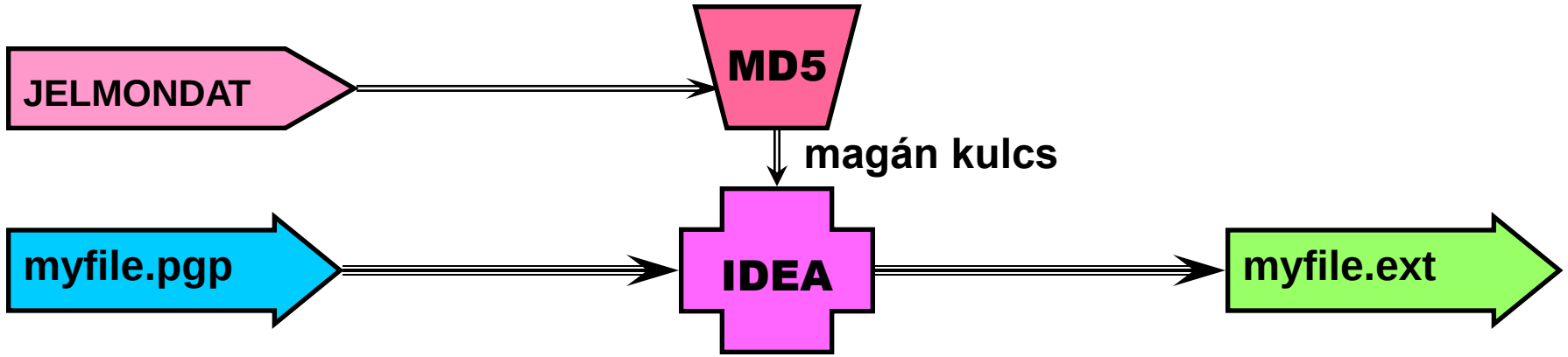
Peter Gutmann: Cryptography and Data Security, University of Auckland, New Zealand, Course Handout

PGP: SZIMETRIKUS KULCSÚ REJTJELZÉS

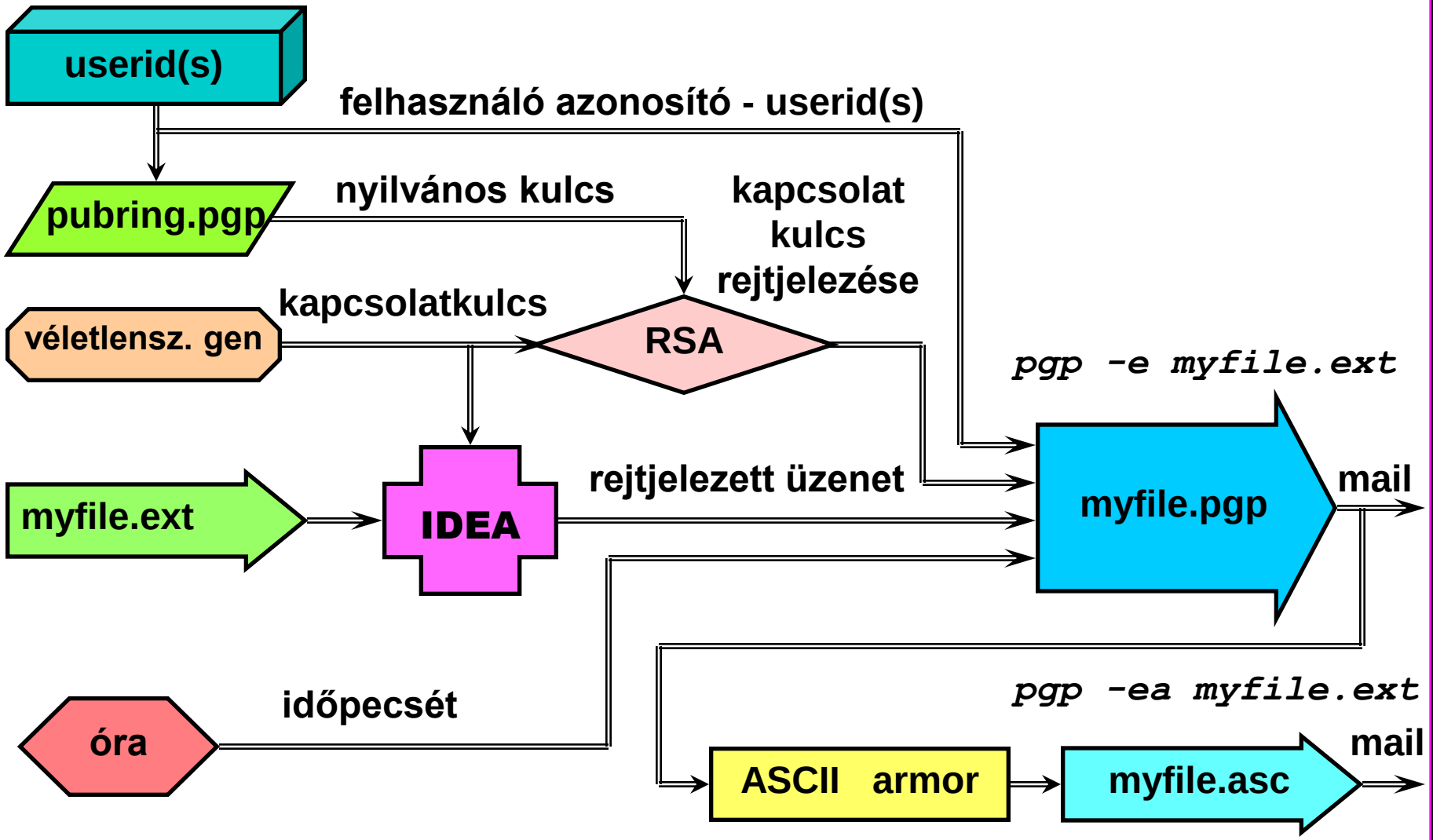
REJTJELZÉS IDEA-val: `pgp -c myfile.ext`



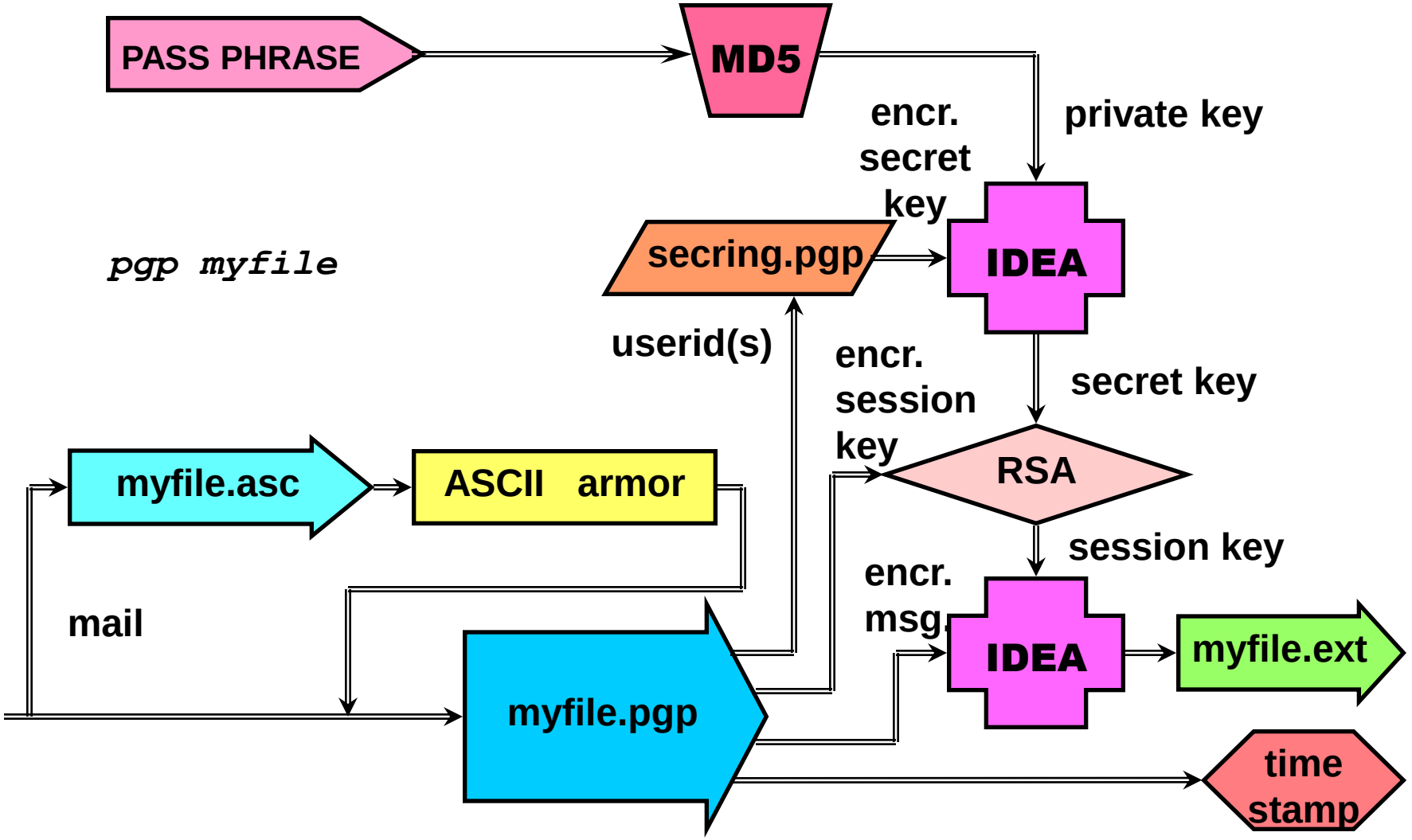
MEGOLDÁS IDEA-val : `pgp myfile`



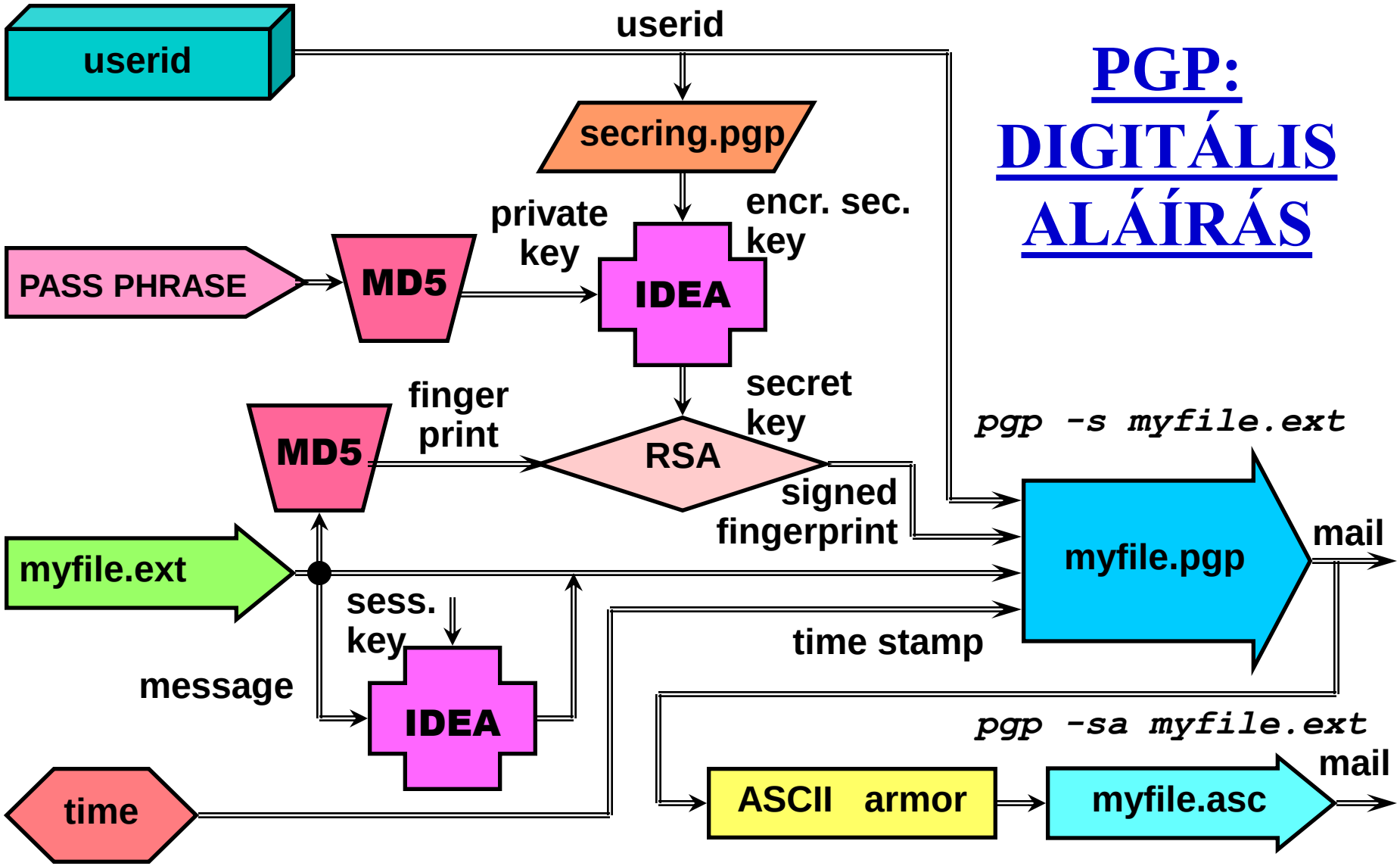
PGP: REJTJELEZÉS és KULCSCSERE



PGP: MEGOLDÁS KULCSCSERÉVEL

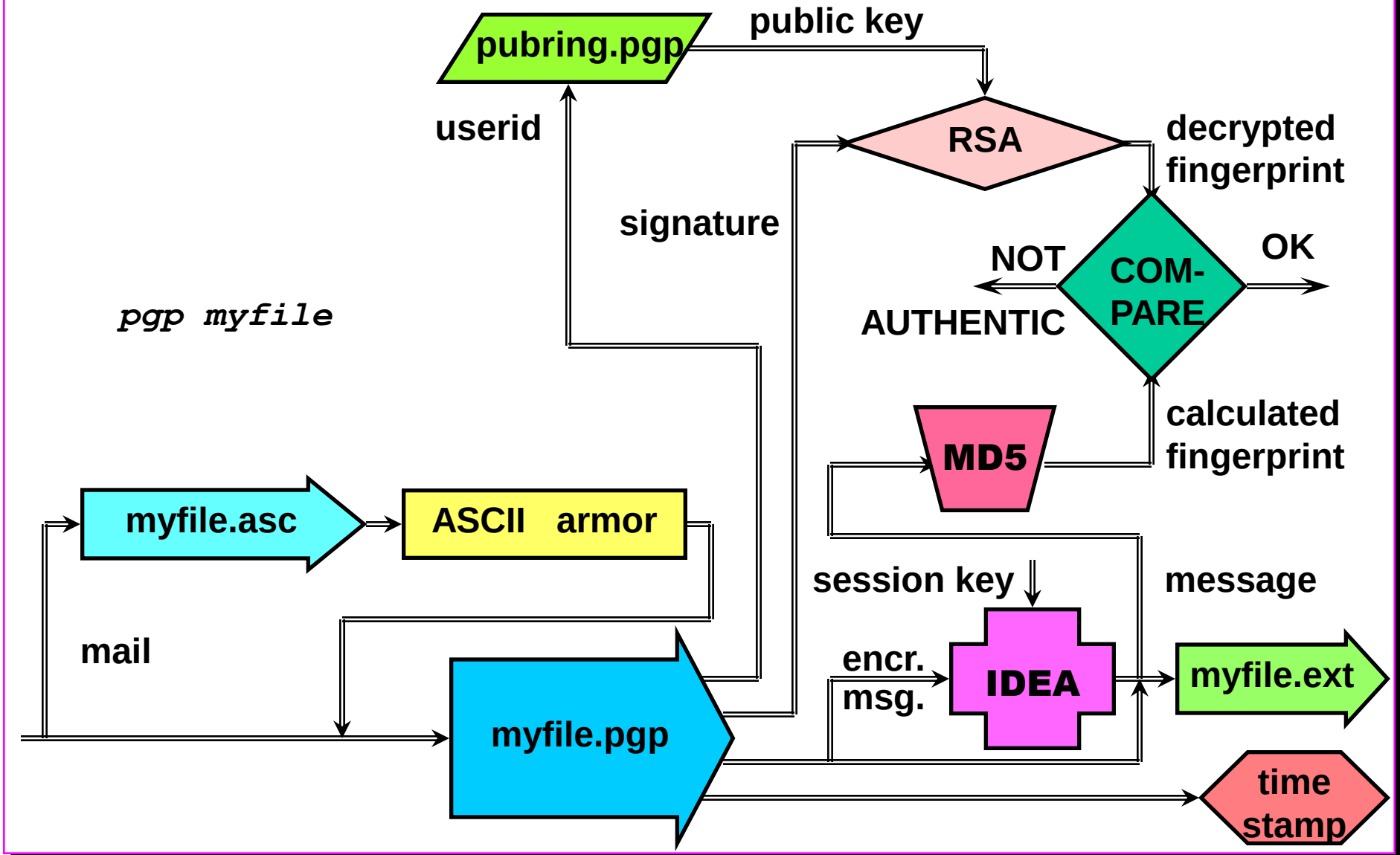


PGP: DIGITÁLIS ALÁÍRÁS



`pgp -sae myfile.ext:` additional encryption of the message in ASCII format

PGP: DIGITÁLIS ALÁÍRÁS ELENŐRZÉSE



ANONYMOUS DIGITAL MONEY with CHEATER IDENTIFICATION - 1

BIT COMMITMENT PROTOCOL:

RUS: *19A5F2D569B0129EF493FA55*

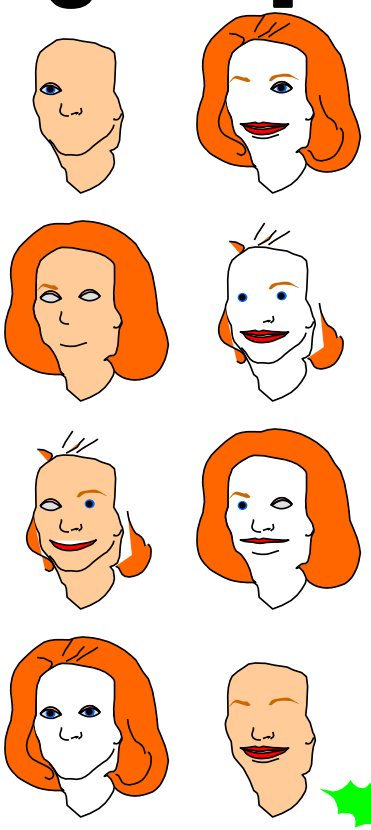
AMOUNT: $1000

POST BANK
01125I2002
AMBERG

IDENTITY STRING PAIRS

$I_{I,k} = \{I_{I,k,L}, I_{I,k,R}\}$

(SECRET SPLITTING)



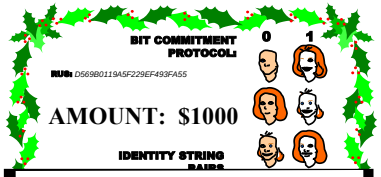
b o r ,

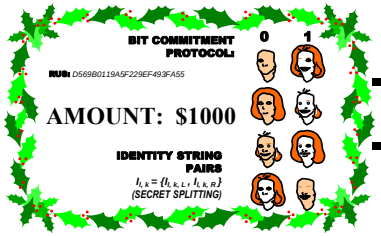
ANONYMOUS DIGITAL MONEY with CHEATER IDENTIFICATION - 2

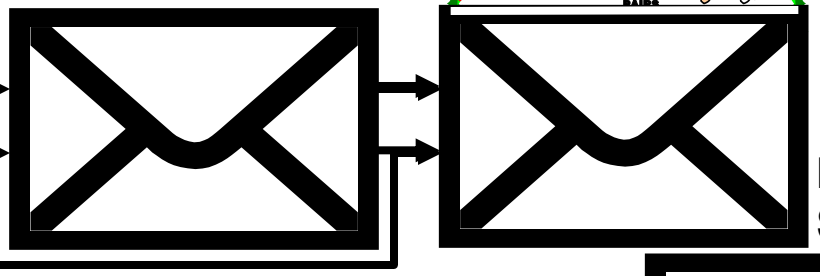
PREPARATION of *N* MONEY ORDER

BLINDING

CUT and CHOOSE PROTOCOL



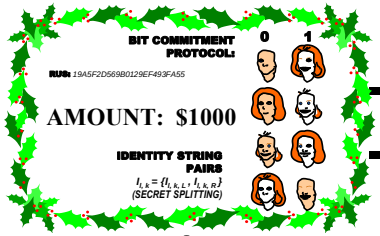


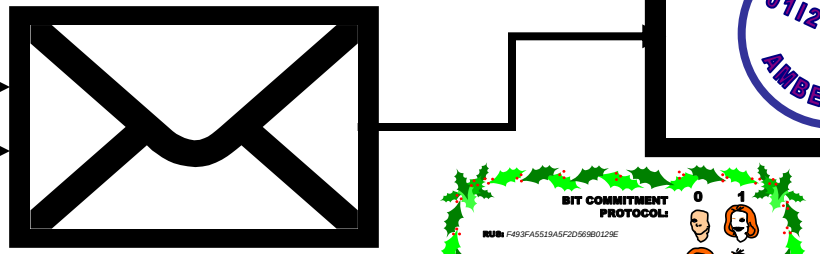


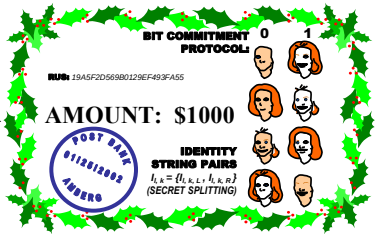
BLIND SIGNATURE

UNBLINDING

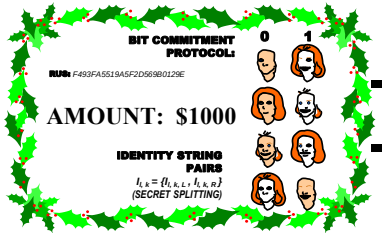
BLINDING FACTOR

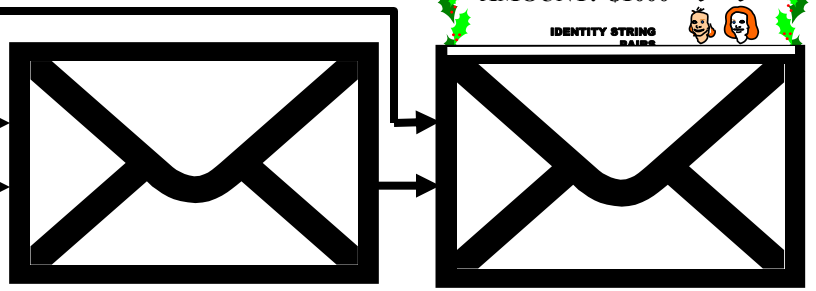






SINGLE SIGNED MONEY ORDER





b o r ,

ANONYMOUS DIGITAL MONEY with CHEATER IDENTIFICATION - 3

BIT COMMITMENT PROTOCOL 0 1

RUS: 19A5F2D569B0129EF493FA55

AMOUNT: $1000

POST BANK 01125I2002 AMBERG

IDENTITY STRING PAIRS

$I_{I,k} = \{I_{I,k,L}, I_{I,k,R}\}$ (SECRET SPLITTING)

FIRST LEGAL PAYMENT SS = 1001

BIT COMMITMENT PROTOCOL 0 1

RUS: 19A5F2D569B0129EF493FA55

AMOUNT: $1000

POST BANK 01125I2002 AMBERG

IDENTITY STRING PAIRS

$I_{I,k} = \{I_{I,k,L}, I_{I,k,R}\}$ (SECRET SPLITTING)

ANONYMOUS PAYMENT

NO PERSONAL IDENTIFICATION POSSIBLE

DOUBLE SPENDING

RANDOM SELECTOR STRING SS = 1011

THE BANK CHECKS the **RUS** IN DATABASE

BANK

CHEATER IDENTIFICATION

after DOUBLE SPENDING

BIT COMMITMENT PROTOCOL 0 1

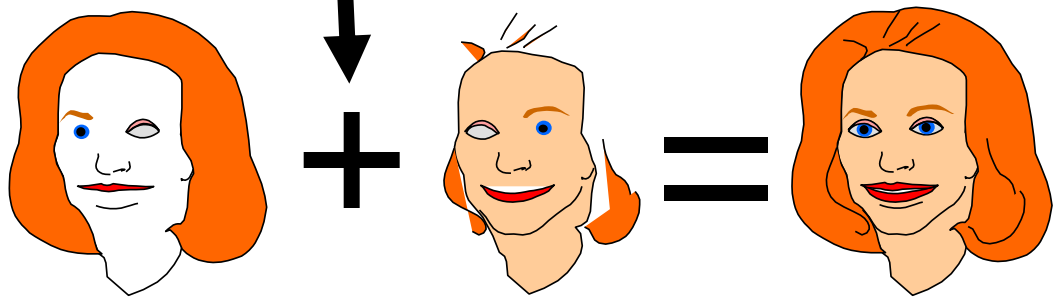
RUS: 19A5F2D569B0129EF493FA55

AMOUNT: $1000

POST BANK 01125I2002 AMBERG

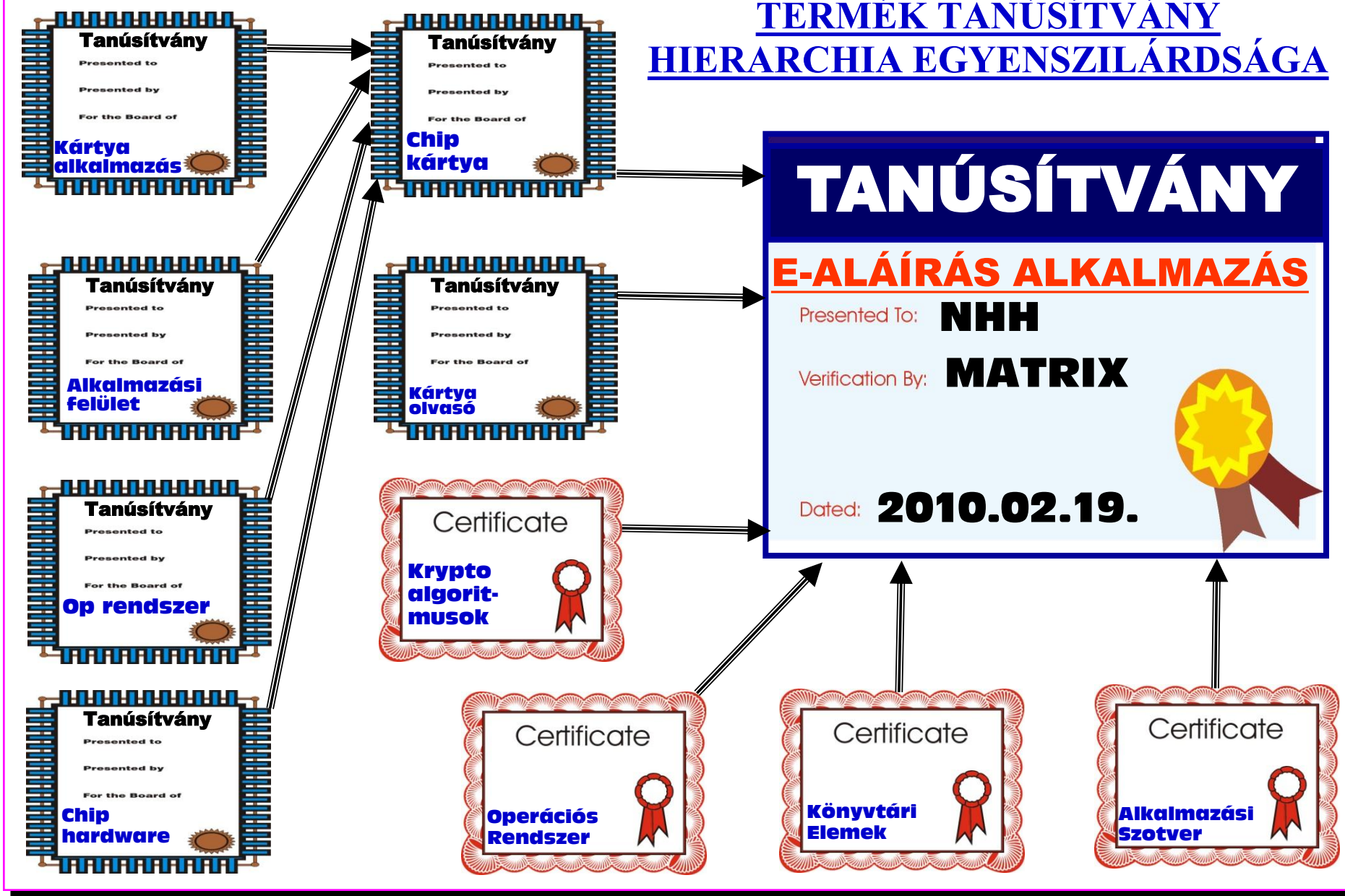
IDENTITY STRING PAIRS

$I_{I,k} = \{I_{I,k,L}, I_{I,k,R}\}$ (SECRET SPLITTING)



b o r ,

TERMÉK TANÚSÍTVÁNY HIERARCHIA EGYENSZILÁRDSÁGA



ELEKTRONIKUS KORMÁNYZAT LEGFONTOSABB BIZTONSÁGI KÖVETELMÉNYEI 1.

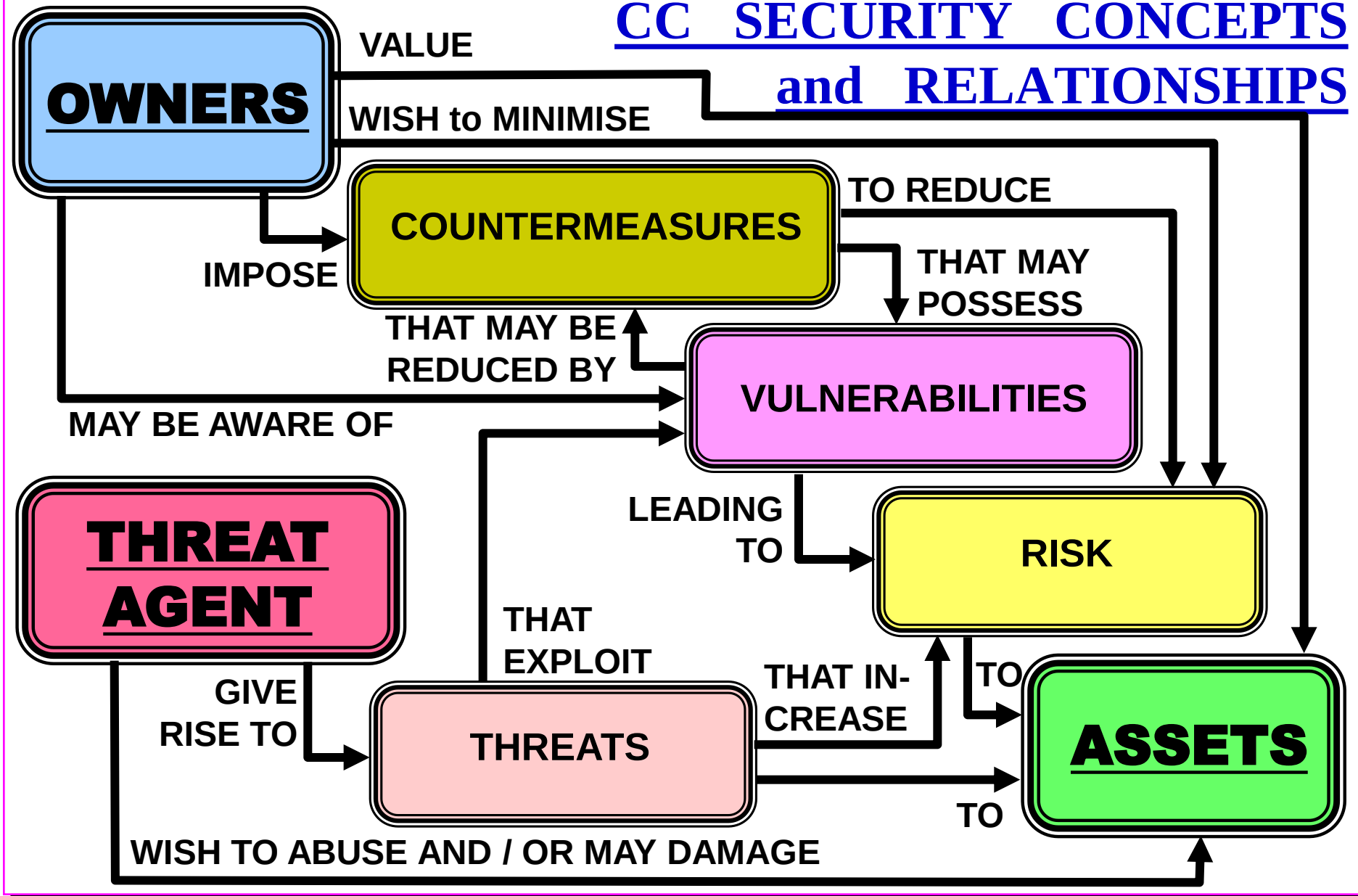
http://www.fogalomtar.hu/

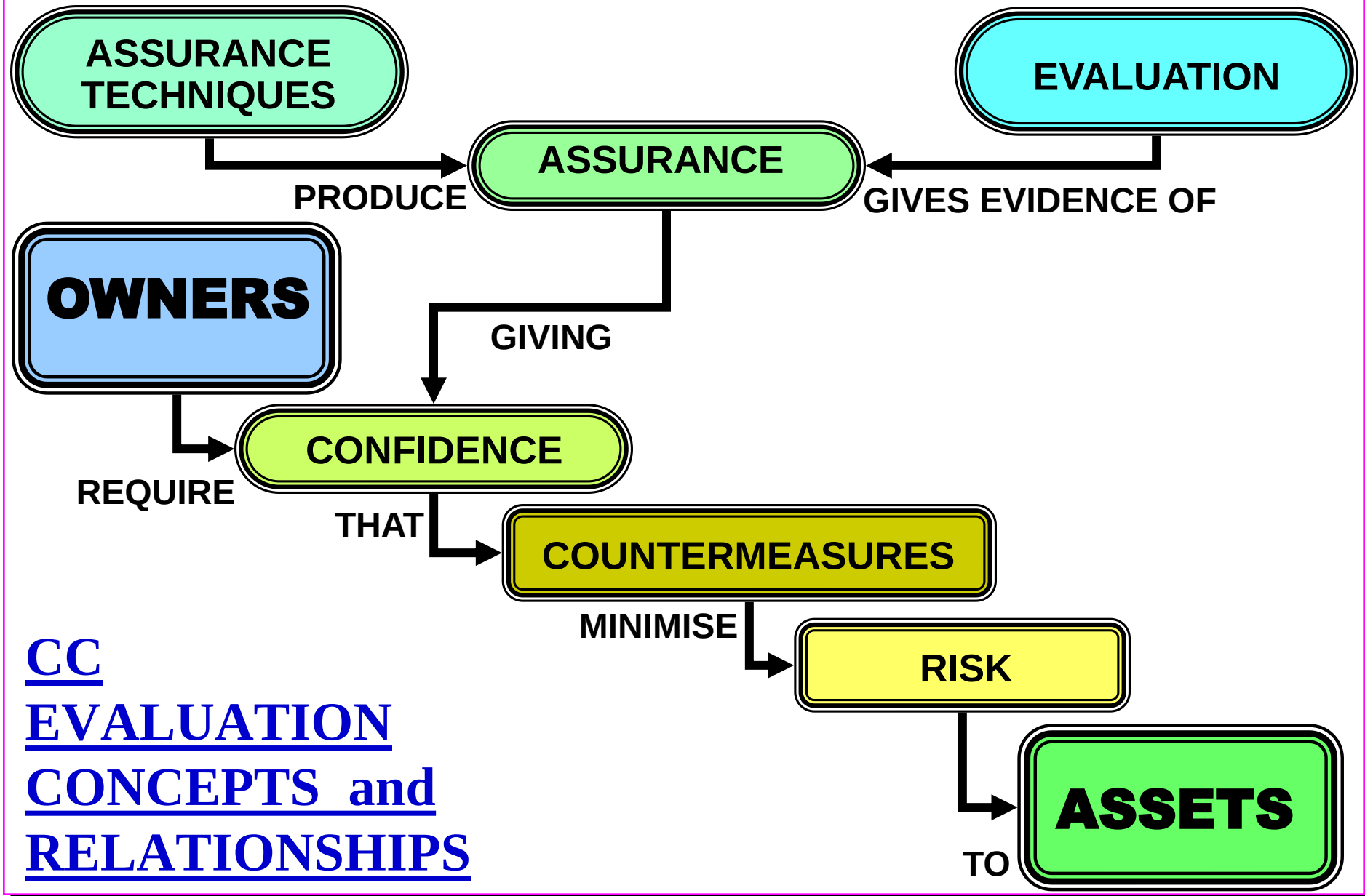
Bizalmasság Confidentiality Vertraulichkeit	Az információk vagy adatok esetében a bizalmasság azt jelenti, hogy azokhoz csak az arra jogosítottak és csak az előírt módokon férhetnek hozzá, és nem fordulhat elő úgynevezett jogosulatlan információszerzés. Ez vonatkozhat programokra, mint szélesebb értelemben vett információkra is.
Sértetlenség Integrity Integrität	A sértetlenséget általában az információkra, adatokra, illetve a programokra értelmezik. Ez az alap-veszélyforrás a programokat is érinti, mivel az adatok sértetlenségét csak rendeltetésszerű feldolgozás és átvitel esetén lehet biztosítani. A sértetlenség fogalma alatt gyakran értik a sérthetetlenségen túli teljességet, továbbá az ellentmondás mentességet és a helyességet, együttesen: adat-integritást. Az integritás ebben az összefüggésben azt jelenti, hogy az információ valamennyi része rendelkezésre áll és elérhető.
Hitelesség Authenticity Authentizität	A hitelesség (adatok esetében) az adat olyan biztonsági tulajdonsága, amely arra vonatkozik, hogy az adat (bizonyíthatóan) egy elvárt forrásból származik. Ehhez az szükséges, hogy az informatikai kapcsolatban lévő partnerek kölcsönösen (és egyértelműen) felismerjék egymást, és ez az állapot a kapcsolat teljes ideje alatt fennálljon.
Rendelkezésre állás Availability Verfügbarkeit	Rendelkezésre álláson azt a valószínűséget értjük, amellyel egy meghatározott időintervallumon belül az informatikai rendszer a tervezésekor meghatározott funkcionalitásnak megfelelően, a feljogosított felhasználók által használható, azaz a rendszer működőképessége sem átmenetileg, sem pedig tartósan nincs akadályozva.

ELEKTRONIKUS KORMÁNYZAT LEGFONTOSABB BIZTONSÁGI KÖVETELMÉNYEI 2.

Partnerazonosság Authenticity Authentizität	A kapcsolat idejére, például SSL/TLS
Megőrzési idő Retention period Aufbewahrungs-fristen	Bizonyító erejű hiteles megőrzés és archiválás.
Meghatározhatóság Definiteness Bestimmtheit	Sértetlenség, hitelesség (eredet) vagy a dokumentum keletkezési, elküldési, megérkezési, feldolgozási stb. idejének meghatározhatósága. Például: Időpecsét.
Hiteltérdemlőség Vertrauenswürdigkeit Trustworthiness	Az a szint amennyire egy termékről, vagy szolgáltatásról elhihető, hogy a meghirdetett biztonsági funkciókkal rendelkezik. Alapja lehet a gyártó nyilatkozata, vagy független vizsgáló, ellenőrző és tanúsító szervezet jogkövetkezményekkel járó nyilatkozata.

CC SECURITY CONCEPTS and RELATIONSHIPS





CC EVALUATION CONCEPTS and RELATIONSHIPS

COBIT

BUSINESS OBJECTIVES

IT GOVERNANCE

COBIT

INFORMATION

CRITERIA

EFFECTIVENESS EFFICIENCY
CONFIDENTIALITY INTEGRITY
AVAILABILITY COMPLIANCE
RELIABILITY

MONITORING

- M1 MONITOR THE PROCESS
- M2 ASSESS INTERNAL CONTROL ADEQUANCY
- M3 OBTAIN INDEPENDENT ASSUARANCE
- M4 PROVIDE FOR INDEPENDENT AUDIT

DELIVERY & SUPPORT

- DS1 DEFINE and MANAGE SERVICE LEVELS
- DS2 MANAGE THIRD-PARTY SERVICES
- DS3 MANAGE PERFORMANCE and CAPACITY
- DS4 ENSURE PERFORMANCE and CAPACITY
- DS5 ENDURE SYSTEM SECURITY
- DS6 IDENTITY and ALLOCATE COSTS
- DS7 EDUCATE and TRAIN USERS
- DS8 ASSIST and ADVICE CUSTOMERS
- DS9 MANAGE the CONFIGURATION
- DS10 MANAGE PROBLEMS and INCIDENTS
- DS11 MANAGE DATA
- DS12 MANAGE FACILITIES
- DS13 MANAGE OPERATIONS

PLANNING & ORGANISATION

- PO1 DEFINE A STRATEGIC IT PLAN
- PO2 DEFINE THE INFORMATION ARCHITECTURE
- PO3 DEFINE THE TECHNOLOGICAL DIRECTION
- PO4 DEFINE THE IT ORGANIZATION AND RELATIONSHIP
- PO5 MANAGE THE IT INVESTMENT
- PO6 COMMUNICATE MANAGEMENT AIMS AND DIRECTION
- PO7 MANAGE HUMAN RESOURCES
- PO8 ENSURE COMPLIANCE WITH EXTERNAL REQUIREMENTS
- PO9 ASSESS RISKS
- PO10 MANAGE PROJECTS
- PO11 MANAGE QUALITY

ACQUISITION & IMPLEMENTATION

- AI1 IDENTIFY AUTOMATED SOLUTION
- AI2 ACQUIRE AND MAINTAIN APPLICATION SOFTWARE
- AI3 ACQUIRE AND MAINTAIN TECHNOLOGY INFRASTRUCTURE
- AI4 DEVELOP AND MAINTAIN PROCEDURES
- AI5 INSTALL AND ACCREDIT SYSTEM
- AI6 MANAGE CHANGES

IT RESOURCES

PEOPLE
APPLICATION SYSTEMS
TECHNOLOGY
FACILITIES
DATA

COBIT IT PRO-CESSES

COBIT 3rd edition, July 2000: IT Gover-nance Institute

SZÉKELY HIMNUSZ

szövegét Csanády György írta 1921-ben

Ki tudja merre, merre visz a végzet
Göröngyös úton, sötét éjjelen.
Segítsd még egyszer győzelemre néped,
Csaba király a csillag ösvényen.
Maroknyi székely porlik, mint a szikla
Népek harcától zajló tengeren.
Fejünk az ár ezerszer elborítja,
Ne hagyd el Erdélyt, Erdélyt Istenem!

ÉNEKELT, HOSSZÚ VÁLTOZAT:

zenéjét Mihalik Kálmán szerezte

Ki tudja merre, merre visz a végzet
Göröngyös úton, sötét éjjelen.
Segí sd még egyszer győzelemre néped,
Csaba királyfi csillag ösvényen!
Maroknyi székely porlik, mint a szikla
Népek harcának zajló tengerén.
Fejünk az ár, jaj, százszor elborítja,
Ne hagyd elveszni Erdélyt, Istenünk!
Ameddig élünk, magyar ajkú népek,
Megtörni lelkünk nem lehet soha,
Szülessünk bárhol, Földünk bármely pontján
Legyen a sorsunk jó vagy mostoha!
Keserves múltunk - évezredes balsors,
Tatár, török dúlt, a labanc rabigált.
Jussunk e honban, magyar-székelyföldön
Szabad hazában éljünk boldogan!

VÉGE