UNIVERSITY OF AMSTERDAM

Jaap van Ginkel

Security of Systems and Networks

2 September 2024, Part 1 Intro and Traditional Crypto

This Block

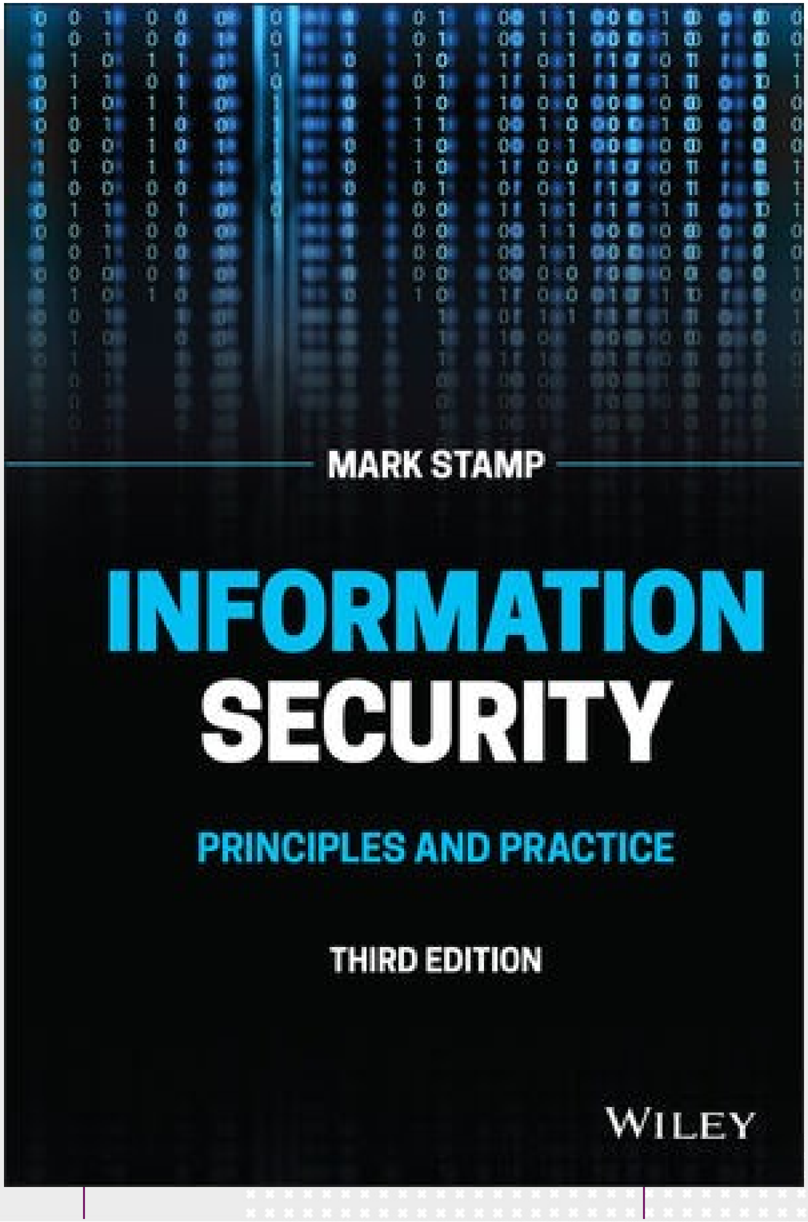
- Monday and Thursday
  - Security of Systems and Networks (SSN)
  - Jaap van Ginkel (Lucas Hecht, Zhiyang Wang)
- Tuesday and Friday
  - Classical Internet systems (CIA)
  - Yuri Demchenko
- Wednesday
  - Colloquium/Extra Lab or project time

Seating and Ergonomics

- At home and in the lab (Instruction by Jaap at 13:00)
- Seating in groups

Book

- Open book exam
- Information Security: Principles and Practice, 3rd Edition
- Mark Stamp
- ISBN: 978-1119505907



MARK STAMP

INFORMATION SECURITY

PRINCIPLES AND PRACTICE

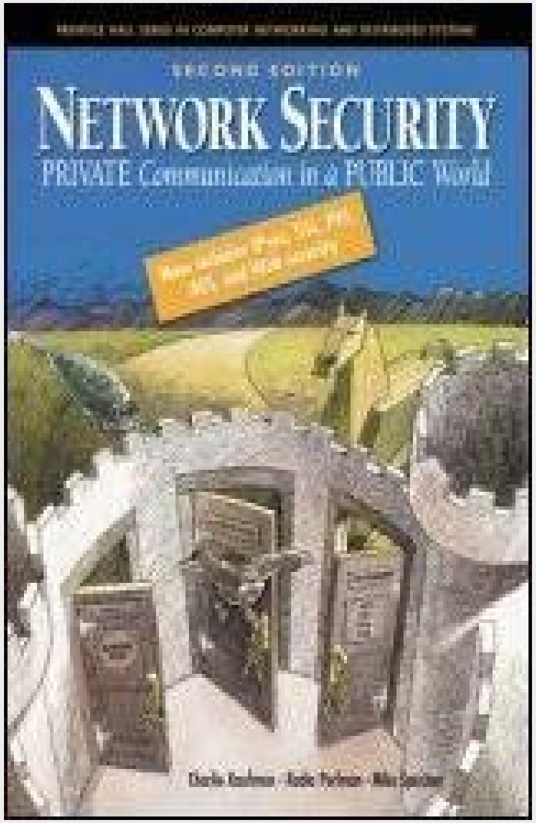
THIRD EDITION

WILEY

Another book

- Network Security: Private Communication in a Public World, 2/E
- Charlie Kaufman
- Radia Perlman
- Mike Speciner

- ISBN-13: 9780130460196


SECOND EDITION
NETWORK SECURITY
PRIVATE Communication in a PUBLIC World
Charlie Kaufman · Radia Perlman · Mike Speciner

SSN specific rules

- Lecture Presence 10:00-12:15

  Lecture starts 10:15-12.xx
- Lab Presence 13:00-16:00
- Presence is mandatory
  - □ Also when you are finished or already know the material
  - □ Report absence beforehand
  - □ If you leave tell the teacher or TA
- All mail for SSN to

  SSN.teachers@os3.nl

Labs

- Maintain your Logs !
- Work in different groups for each assignment
- Make sure you show your own input in group work
- Do not copy please...

WIKI

- https://www.os3.nl/2024-2025/courses/ssn/start
- UvA learning systems (Canvas) only for grades
- Datanose and SIS only for formal registration of courses

Security & Network Engineering

Trace: • Schedule 2019-2020 • Security of Systems and Networks

Security of Systems and Networks

Lecturer	Jaap van Ginkel
Lab teachers	Arno Bakker

Your own contribution to SSN

- Ask questions
- Debate topics with each other
- If there is a SSN subject you are an expert at...
- And you have the time to prepare a presentation...
- Let me know

Guest lecturers (TBD)

Karst Koymans - Crypto math
Jan Joris Vereijken - Security by Design
Possibly lectures
Post quantum crypto algortims DJB
Cipher machines
Quantum Crypto

House rules

- Guest lectures
  - Be inquisitive/critical
  - Be polite
  - Don't use your laptop or PC
  - Presence mandatory
- Jaap
  - You can use your laptop PC for SSN related work
  - Presence mandatory

SSN Project

- Preparation for RP1
- More fun than lab exercises
- You will get graded for it...
- Work in groups of 3 (if needed 4)
- Choose a subject in week 3
- Week 1-3 Lab exercises
- Week 4-7 Work on project

Deadlines

- SSN Lab exercises feedback
- SSN Lab exercises corrections
- SSN first project idea 12 September
- SSN final project proposal 19 September
- SSN project presentations 18 October
- SSN project report 27 October
  - Extension only granted if applied week in advance
- All deadlines 23:59 UTC+1

Exam

- Open book
- Save a tree today
- No electronic aids
- Guest lectures and additional materials are part of the exam

Grading

- Presence: Mandatory
- Labs: Conditional to pass
- Project report: 30 %
- Project presentation: 0 %
- Exam: 70 %
- Minimum grade for exam and report 4.0

Possibly:

- Peer review

Film

- Voluntary participation
- Thursday 17:00 ?
- Suggestions
  - The imitation Game/ Enigma
  - Catch me if you can
  - A Beautiful mind
  - Mr Robot
  - Breaking the code

Planning SSN

Crypto History

□ Cryptology

□ Transposition Substitution

□ Frequency analysis

□ Vigenère

□ Enigma

Authentication

- □ AuthN/Authz
- □ SSO
- □ Kerberos
- □ A-Select
- □ Shibboleth
- □ Biometrics

Passwords

- Cracking
  - Hashcat/John
  - Distributed cracking
  - Rainbow tables
  - Hashes

Practical security

□ Firewalls

□ Wrappers

□ Port knocking

□ SSH SCP

□ LDAP

□ Windows/Unix/Mac

Social Engineering

- Soft side of security

SSL/TLS

- □ Versions
- □ Ciphers
- □ Implementation
- □ MITM attacks

Smartcards

- Javacard
- GSM, RSA
- OpenPGPcard
- Guest lecture by Riscure

Email security

- PGP
- S/MIME X.509

PKI

- □ Public key cryptography
- □ Trust models
- □ Revocation
- □ Key management
- □ Dutch Diginotar Debacle

IP-SEC

- Design and modes
- IKE/Skip
- Practical Implementations

How knowledgeable do you consider yourself in these SSN topics?

1) Total Newbie
2) I know some of the topics
3) I have followed a course before
4) I know most of the topics in detail
5) I could deliver this course

Traditional Crypto

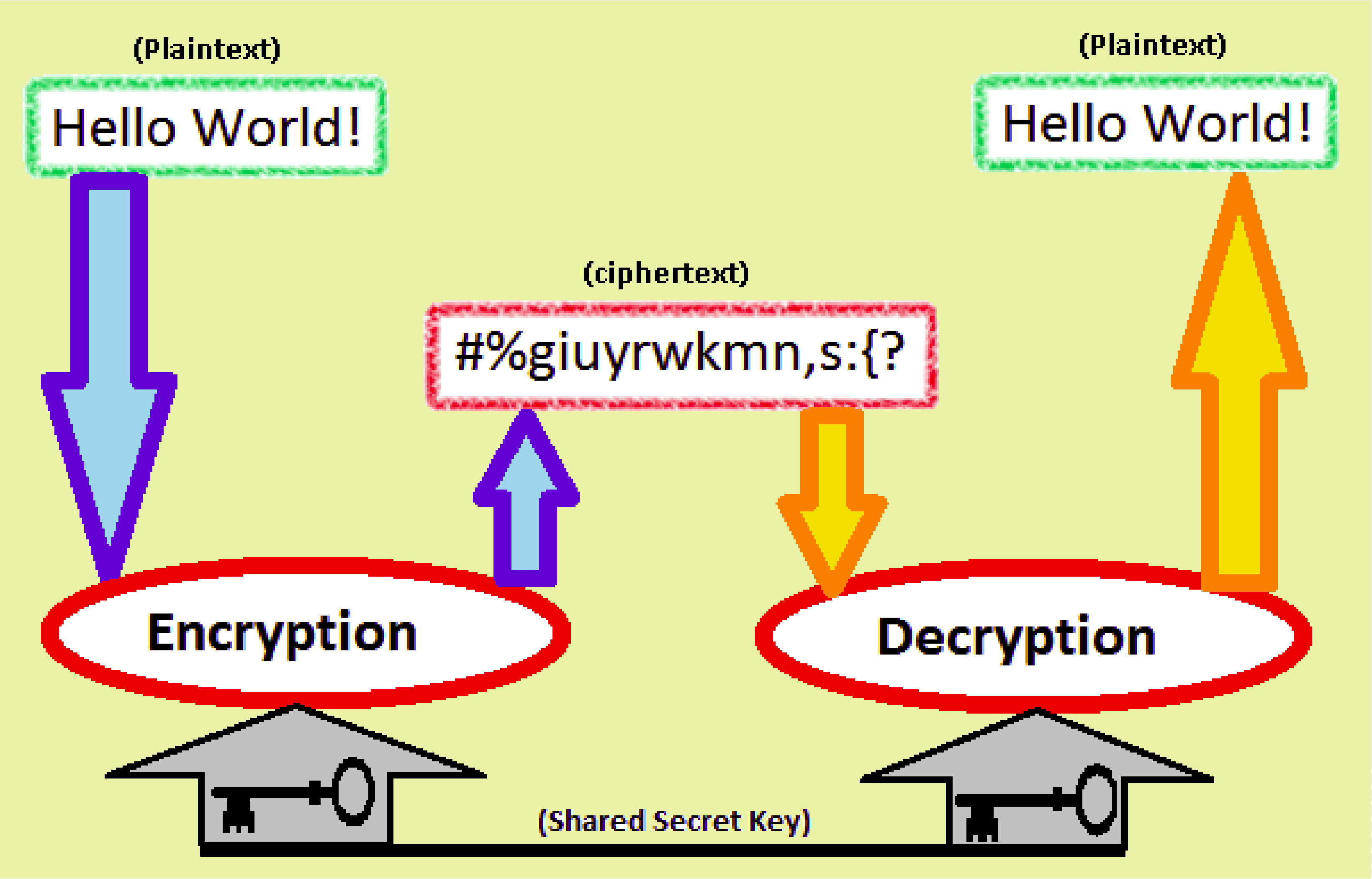
Cryptology

- Cryptography
  - Greek kryptós, "hidden", and gráphein, "to write"
- Cryptanalysis
  - Greek kryptós, "hidden", and analýein, "to loosen" or "to untie")

Crypto

- **Cryptology** The art and science of making and breaking “secret codes”
- **Cryptography** making “secret codes”
- **Cryptanalysis** breaking “secret codes”
- **Crypto** all of the above (and more)

Schematic


(Plaintext)
Hello World!
(Plaintext)
Hello World!
(ciphertext)
#%giuyrwkmn,s:{?
Encryption
Decryption
(Shared Secret Key)

How to Speak Crypto

- A *cipher* or *cryptosystem* is used to *encrypt* the *plaintext*
- The result of encryption is *ciphertext*
- We *decrypt* ciphertext to recover plaintext
- A *key* is used to configure a cryptosystem
- A *symmetric key* cryptosystem uses the same key to encrypt as to decrypt
- A *public key* cryptosystem uses a *public key* to encrypt and a *private key* to decrypt

Crypto

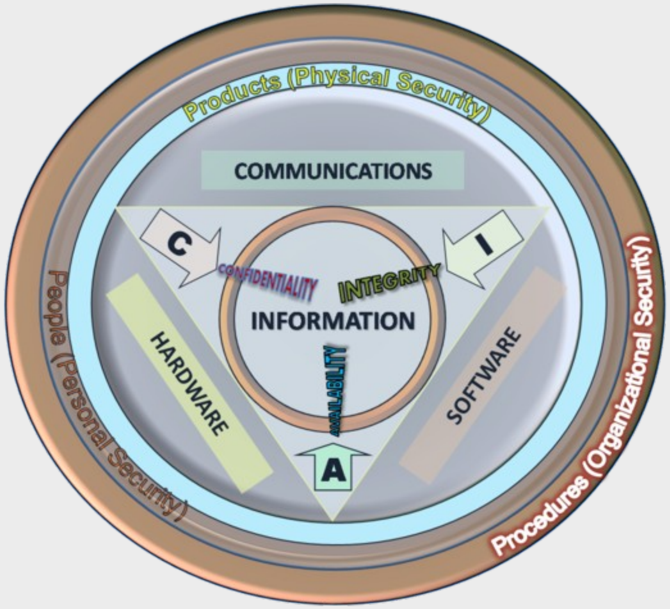
- Basic assumptions
  - The system is completely known to the attacker
  - Only the key is secret
  - That is, crypto algorithms are not secret
- This is known as **Kerckhoffs' Principle**
- Why do we make this assumption?
  - Experience has shown that secret algorithms are weak when exposed
  - Secret algorithms never remain secret
  - Better to find weaknesses beforehand

Definitions

- A *cipher* or *crypto system* is used to encrypt a *plaintext*
- The result is a *ciphertext*
- A *decrypt* gives the plaintext
- A *Key* is the configuration of the cipher

Information Security

- Confidentiality
- Integrity
- Availability


Products (Physical Security)
COMMUNICATIONS
C
I
CONFIDENTIALITY
INTEGRITY
INFORMATION
AVAILABILITY
A
HARDWARE
SOFTWARE
People (Personal Security)
Procedures (Organizational Security)

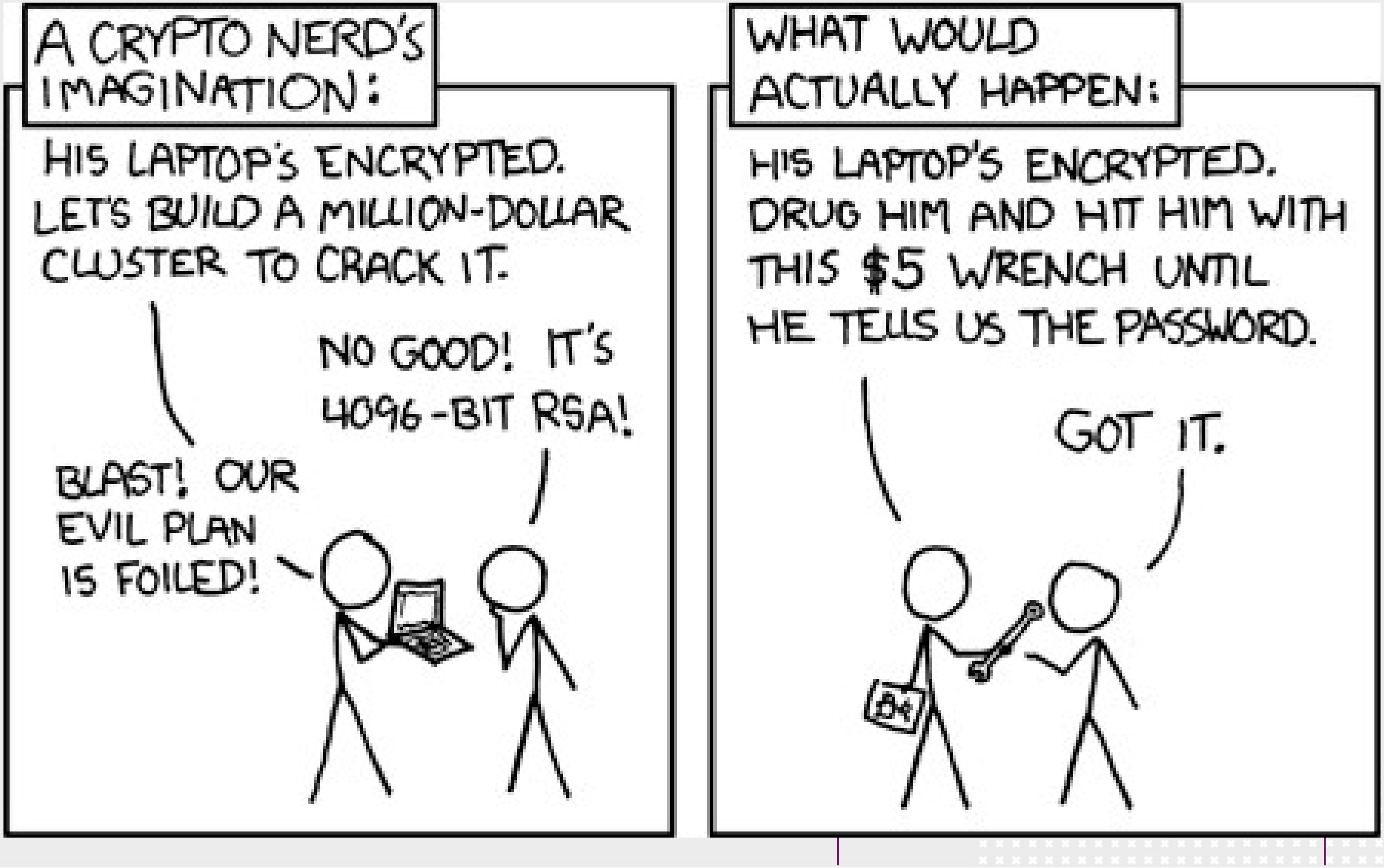
More models

- Possession or Control
- Authenticity
- Utility

- Access Control
  - Authentication
  - Authorization

Use of Encryption

- Non-repudiation
- Anti-replay
- Proof of delivery
- Deniable Encryption


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.

Auguste Kerckhoffs

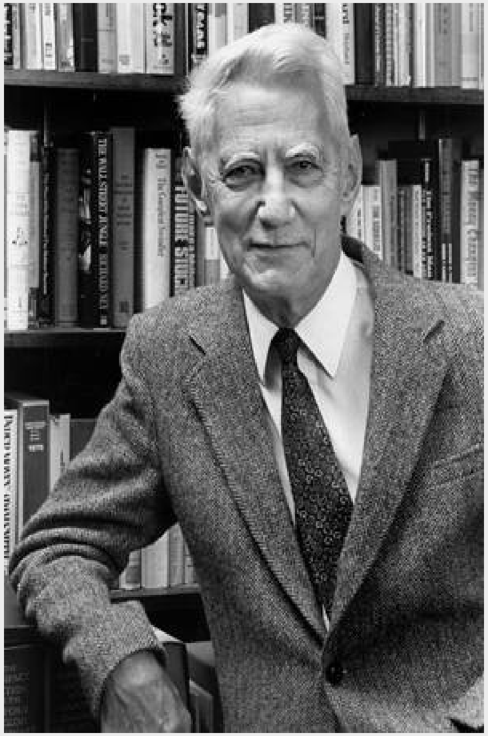
- 1835-1903
- Dutch Linguist and Cryptographer
- Professor at HEC Paris
- La Cryptographie Militaire
- “A cryptosystem should be secure even if everything about the system, except the key, is public knowledge”
- No Security by obscurity

Kerckhoffs ideas

- Le système doit être matériellement, sinon mathématiquement, indéchiffrable ;
- Il faut qu'il n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi
- La clef doit pouvoir en être communiquée et retenue sans le secours de notes écrites, et être changée ou modifiée au gré des correspondants ;
- Il faut qu'il soit applicable à la correspondance télégraphique ;
- Il faut qu'il soit portatif, et que son maniement ou son fonctionnement n'exige pas le concours de plusieurs personnes ;
- Enfin, il est nécessaire, vu les circonstances qui en commandent l'application, que le système soit d'un usage facile, ne demandant ni tension d'esprit, ni la connaissance d'une longue série de règles à observer.

Claude Shannon

- 1916-2001
- Founder of Information Theory
- The enemy knows the system (Shannon's maxim)
- Confusion and diffusion
  - □ **Confusion** — obscure relationship between plaintext and ciphertext
  - □ **Diffusion** — spread plaintext statistics through the ciphertext
  - □ Proved that one-time pad is secure.

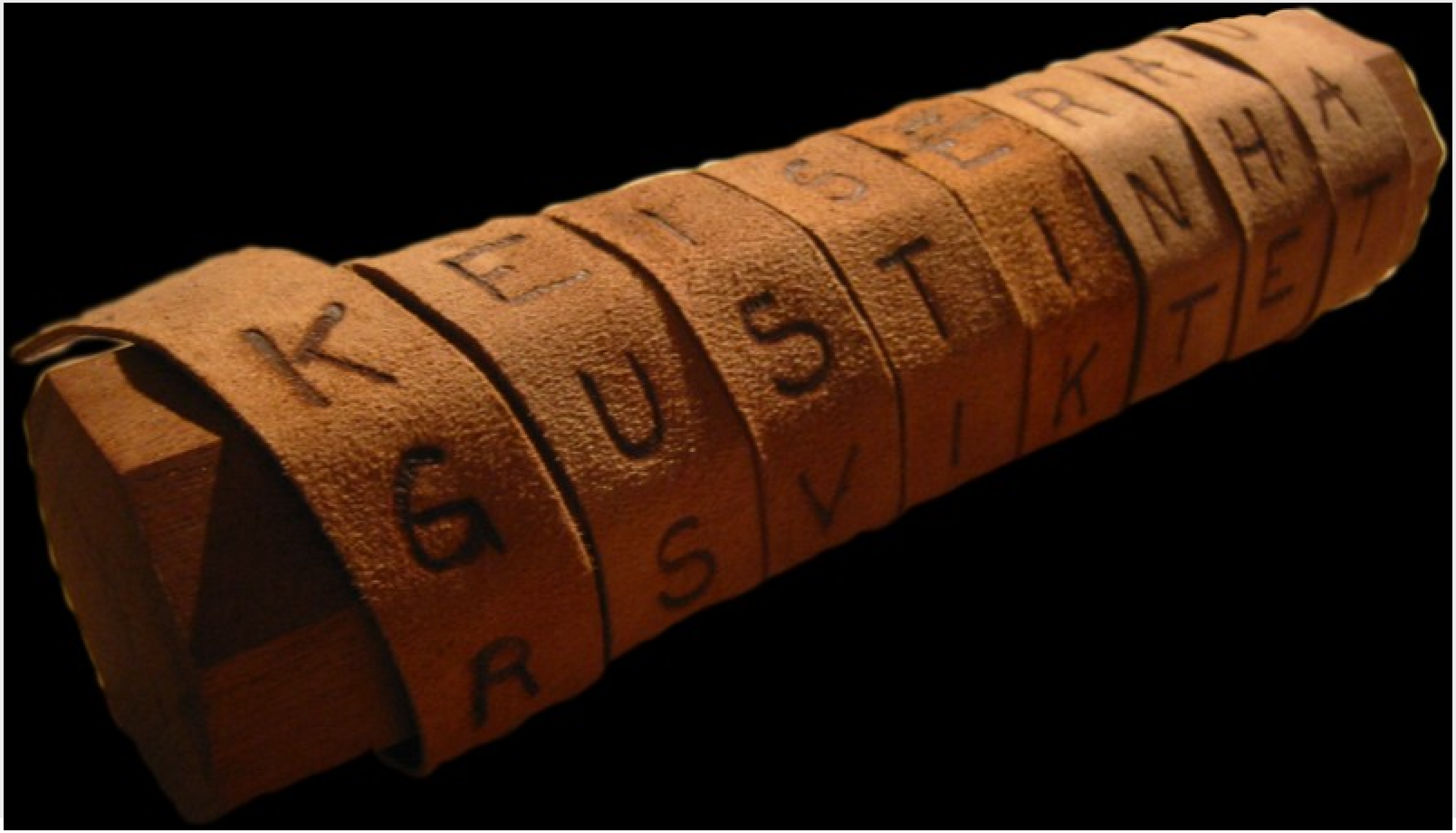


What do you see ?

- HENTEIDTLAEAPMRCMUAK

```
|   | H | E | L | P | M |
|   | E | I | A | M | U |
| N | D | E | R | A |   |
| T | T | A | C | K |   |
|   |   |   |   |   |   |
```

Scytale

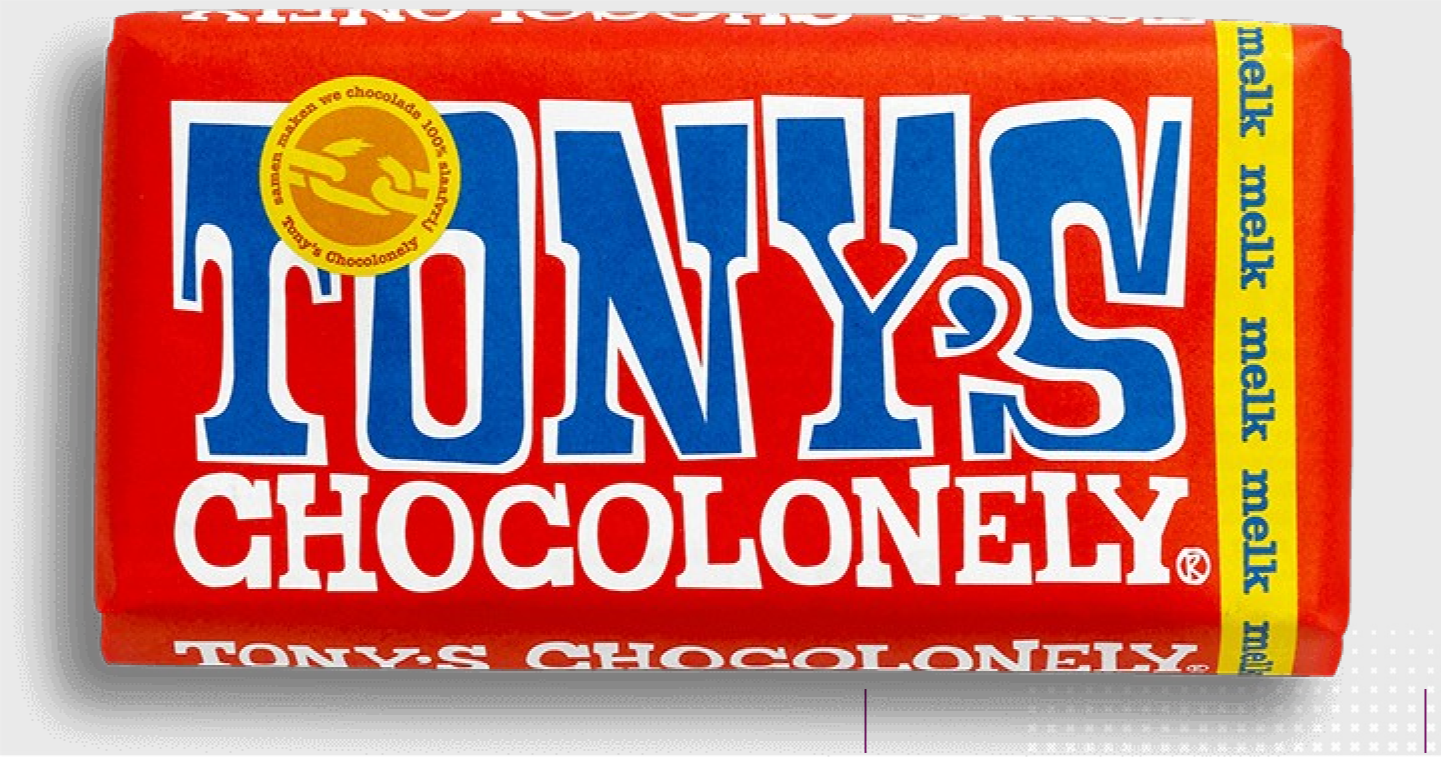


Substitution and Transposition

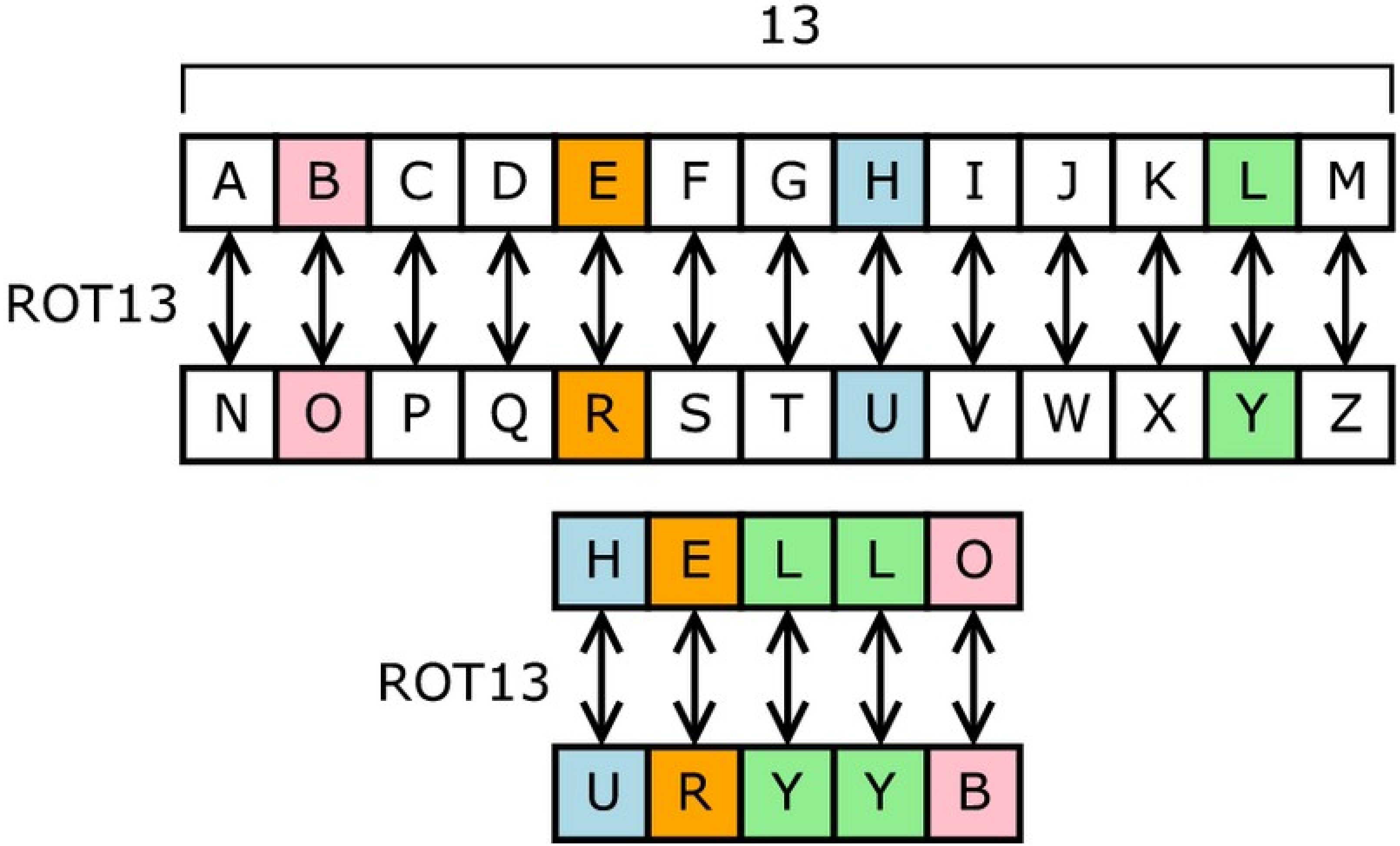
- Transposition
  - Order of the letters is changed
- Substitution
  - Letters are replaced

What do you see?

gjragl lrnef bs far guvf vf tbvat gb or n sha lrne



ROT-13



13

	A	B	C	D	E	F	G	H	I	J	K	L	M
ROT13													
	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

	H	E	L	L	O
ROT13					
	U	R	Y	Y	B

ROT-13/CEASAR

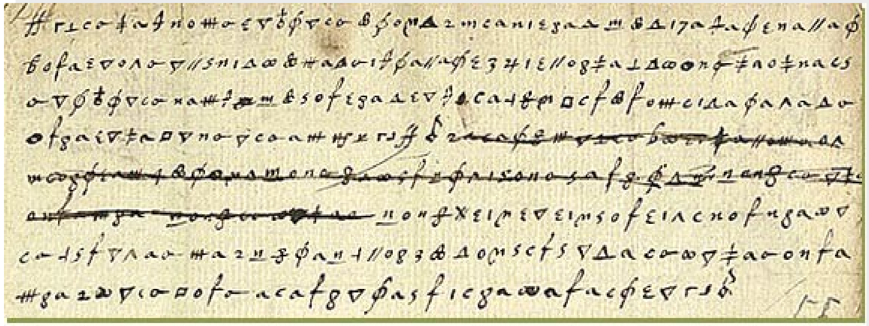
- Only 26 possibilities!
- Exhaustive key search takes microseconds
- Obfuscation
- How to improve?

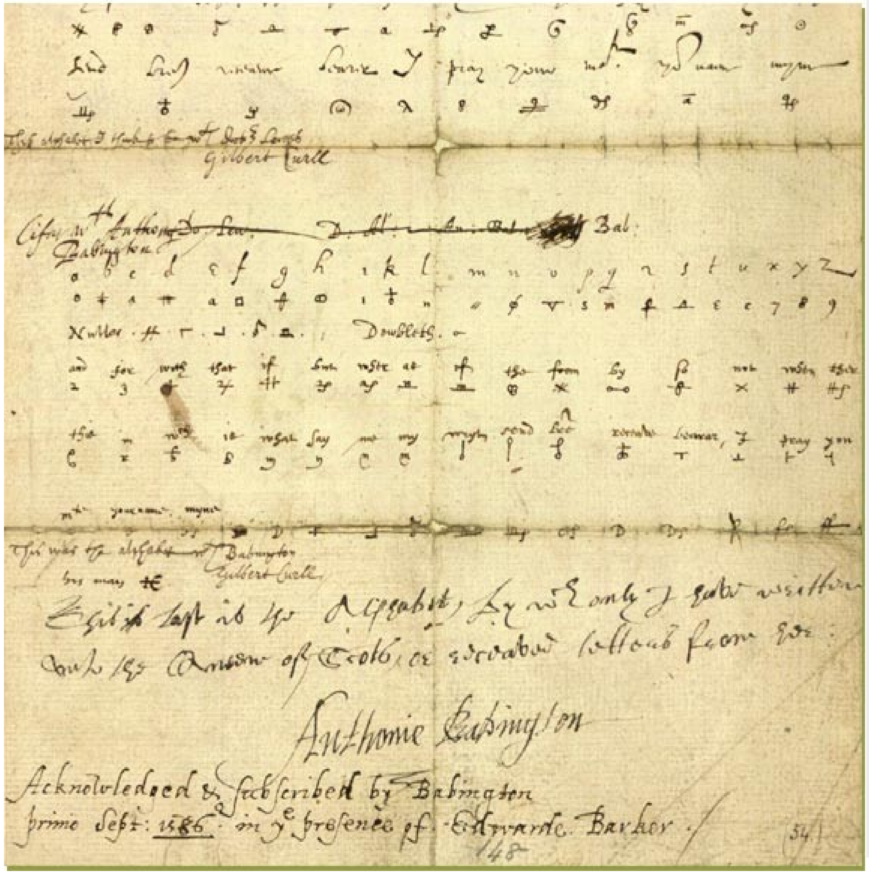
Ceasar's Cipher Decryption

- Suppose we know a Ceasar's cipher is being used:

Plaintext	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Ciphertext	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

- Given ciphertext: VSRQJHEREVTXDUHSDQWV
- Plaintext: spongebobsquarepants





And last remain sure I pray you mr yr name myne

This alphabet I think to be wth the Scots Queen
Gilbert Curll

Cifer wth ~~Anthony~~ Babington ~~[illegible]~~ Bal:

a b c d e f g h i k l m n o p q r s t u x y z

Nulles. Doublets.

and for with that if but where as of the from by so not when there

this in wch is what say me my myne send her receive bearer, I pray you

mr yor name myne

This was the alphabet wth Babington
Gilbert Curll

This is the Alphabet, by wch only I have written
unto the Queen of Scots, or received letters from her:

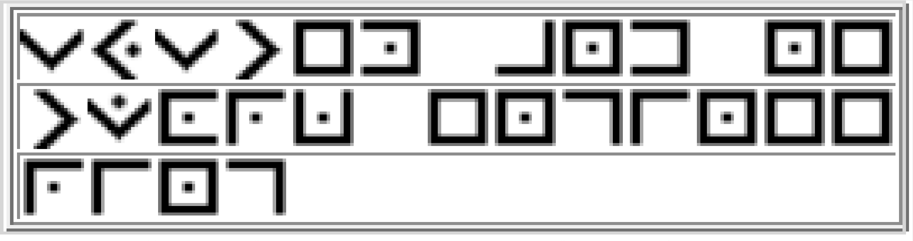
Anthonie Babington

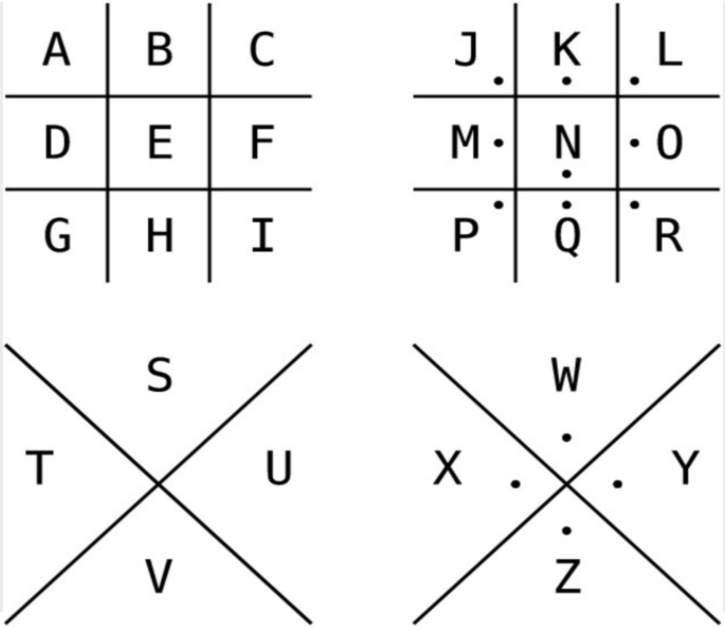
Acknowledged & subscribed by Babington
primo Sept: 1586 in ye presence of Edwarde Barker

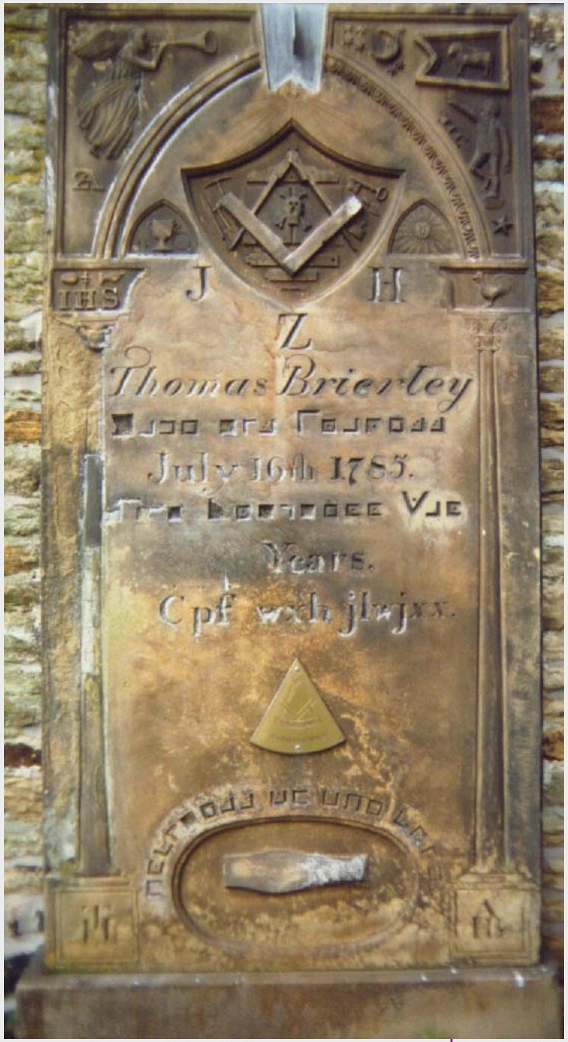
148

(54)

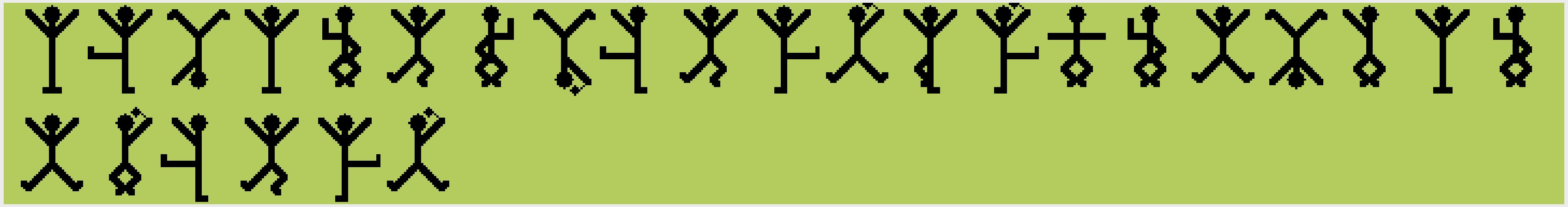
Pigpen / Freemasons







Sherlock Holmes Dancing men Cipher



Simple Substitution

- Plaintext: fourscoreandsevenyearsago
- Key:

Plaintext	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Ciphertext	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

- Ciphertext: IRXUVFRUHDQGVHYHQBHDUVDJR
  - Shift by 3 is “Caesar’s cipher”

Least-Simple Simple Substitution

- In general, simple substitution key can be any **permutation** of letters
  - Need not be a shift
- For example

Plaintext	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Ciphertext	J	I	C	A	X	S	E	Y	V	D	K	W	B	Q	T	Z	R	H	F	M	P	N	U	L	G	O

Monoalphabetic substitution

What do you see?

Sqzof: Qsaofrxl; e. 801–873 QR) vql q Dxlsod hgsndqzi qezoct ql q hiosglghitk, dqzitdqzoeoqf, hinloeoqf, qfr dxloe zitgkolz. Qs-Aofro vql zit yoklz gy zit Olsqdoe htkohqztzoe hiosglghitkl, qfr ol iqostr ql zit "yqzitk gy Qkqw hiosglghin".[3][4][5]

Qs-Aofro vql wgkf of Axyq qfr trxeqztr of Wquirqr.[6] It wteqdt q hkgdoftfz youxkt of zit Igxlt gy Volrgd, qfr q fxdwtk gy Qwwqlor Eqsohil qhhgofztr iod zg gctkltt zit zkqflsqzogf gy Uktta leotfzoyoe qfr hiosglghioeqs ztbzl ofzg zit Qkqwoe sqfuxqut. Ziol egfzqez vozi "zit hiosglghin gy zit qfeotfzl" (ql Itsstfolzoe hiosglghin vql gyztf ktytkktr zg wn Dxlsod leigsqkl) iqr q hkgygxfr tyytez gf iod, ql it lnfzitlomtr, qrqhztr qfr hkgdgztr Itsstfolzoe qfr Htkohqztzoe hiosglghin of zit Dxlsod vgksr.[7] It lxwltjxtfzsn vkgzt ixfrktrl gy gkouofqs zktqzoltl gy iol gvf gf q kqfut gy lxwptezl kqfuofu ykgd dtzqhinloel, tzioel, sguoe qfr hlneigsgun, zg dtroeoft, hiqkdqegsgun,[8] dqzitdqzoel,

qlzkgfgdn, qlzkgsgun qfr ghzoel, qfr yxkzitk qyotsr zg dgkt hkqezoeqs zghoel soat

Substitution

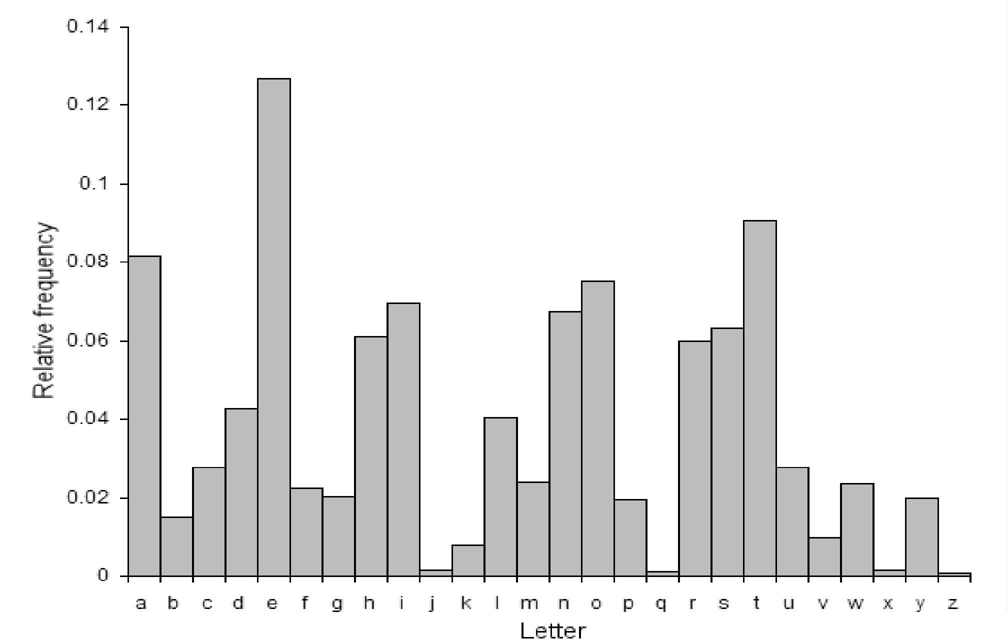
- 26 ! more than 2_{88} possibilities
- Exhaustive search takes ages
- So it is safe ?

Al-Kindi

- أبو يوسف يعقوب ابن إسحاق الكندي
- Abū-Yūsuf Ya’qūb ibn Ishāq al-Kindī (c. 801–873 CE)

Cryptanalysis

- Impossible to search all 2^{88} keys
- Is there a better method ?
- Frequency analysis !



Frequency tables

English:	ETAONIRSHLDCUPFMWYBGVKQXJZ
Dutch:	ENIARDTOGLSHVRMUWJBZCPFXYQ
Esperanto:	AIEONSLTRJUKMPDGCVBFZHQWXY
French:	EANRSITUOLDCMPVBFGHQJZXY
German:	ENIRSADTUGHOLBMCWFKVZPJQXY
Interlingua:	EAILNOSTRUDCMPVGBFHXQJWYZK
Italian:	EAIOLNRTSCDMPUVGZFBHQ
Latin:	IEUTAMSNRODLVCPQBFGXHJKWYZ
Portuguese:	EAOSIDRTNCPUMLVFGQHJXZBKWY
Spanish:	EAOSRNIDLCTUMPGWBQVHFZ
Swedish:	AENRTSIOMGKLDVFBCHPUYJXQWZ

Frequency analysis

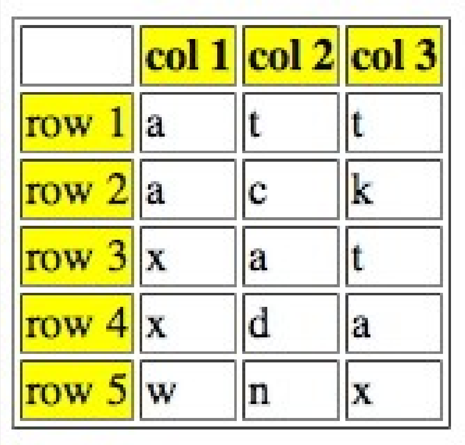
- Language dependent
- Longer text required
- Frequency of letters
- Pairs of letters
- Order of letters

Cryptanalysis: Terminology

- A crypto system is **secure** when the only attack is an “exhaustive search “
- A crypto system is **insecure** when any simplification is known
- Insecure can be safer than secure...

Double Transposition

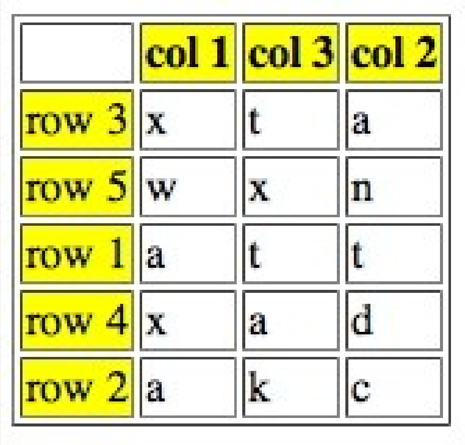
- Plaintext: attackxatxdawn



	col 1	col 2	col 3
row 1	a	t	t
row 2	a	c	k
row 3	x	a	t
row 4	x	d	a
row 5	w	n	x

Permute rows and columns

⇒



	col 1	col 3	col 2
row 3	x	t	a
row 5	w	x	n
row 1	a	t	t
row 4	x	a	d
row 2	a	k	c

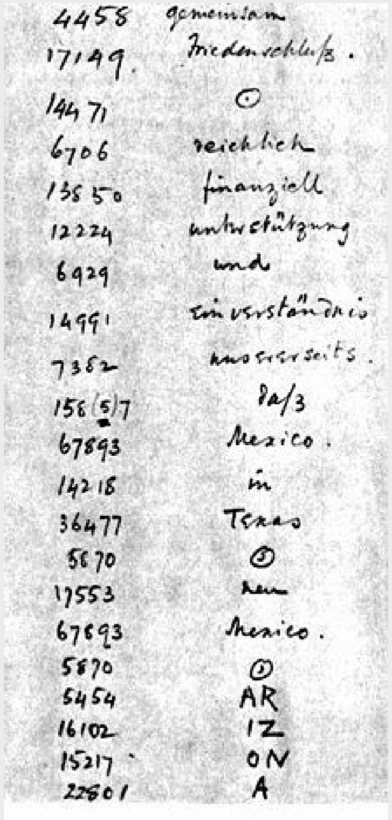
- Ciphertext: xtawxnattxadakc
- Key: matrix size and permutations (3,5,1,4,2) and (1,3,2)

Codebook

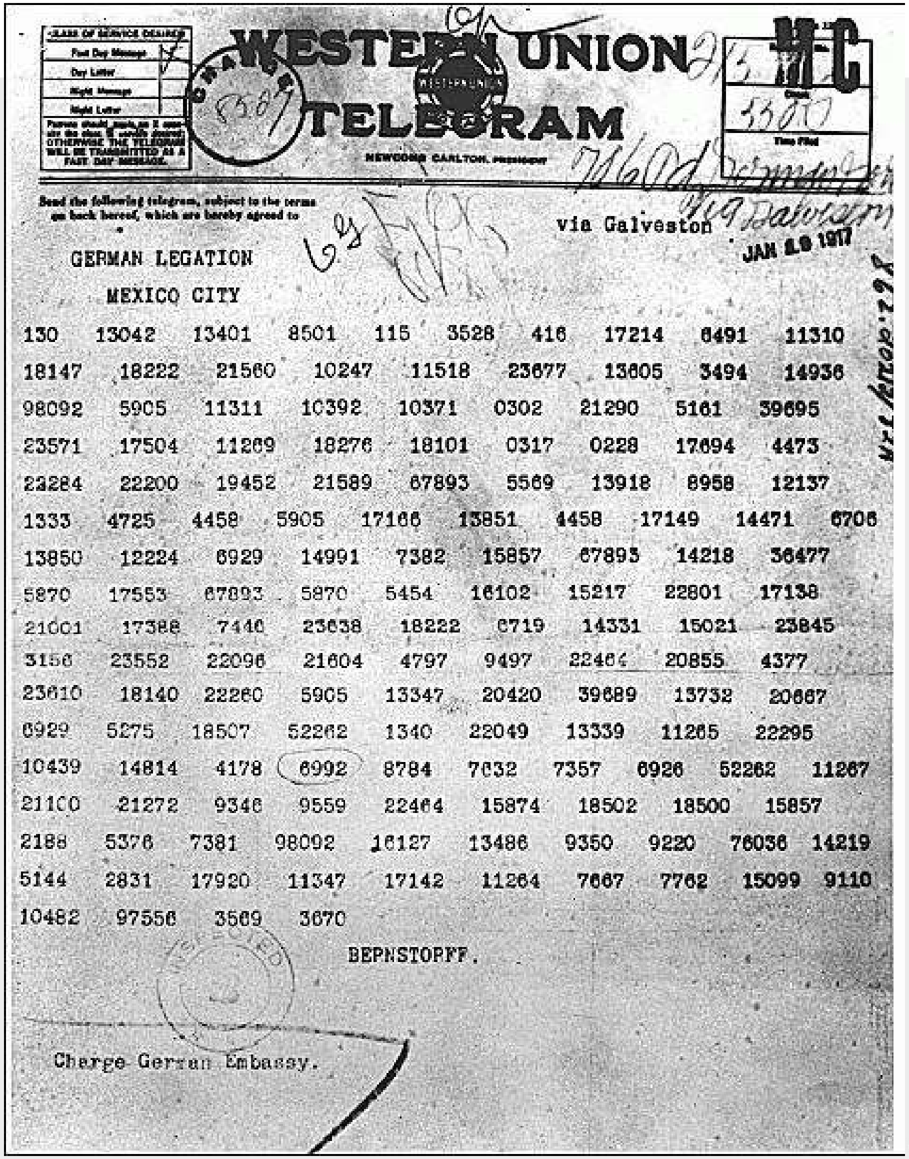
- Literally, a book with "codewords"
- Zimmerman Telegram encrypted with codebook

Februar	13605
fest	13732
finanzielle	13850
folgender	13918
Frieden	17142
Friedenschluss	17149
:	:

Zimmerman Telegram



4458	gemeinsam
17149.	Friedenschluß.
14471	⊙
6706	reichlich
13850	finanziell
12224	unterstützung
6929	und
14991	Einverständnis
7382	unsererseits.
158(5)7	Da/3
67893	Mexico.
14218	in
36477	Texas
5870	⊙
17553	neu
67893	Mexico.
5870	⊙
5454	AR
16102	IZ
15217	ON
22801	A



CLASS OF SERVICE DESIRED
Fast Day Message
Day Letter
Night Message
Night Letter
Patrons should mark an X opposite the class of service desired; OTHERWISE THE TELEGRAM WILL BE TRANSMITTED AS A FAST DAY MESSAGE.

WESTERN UNION TELEGRAM

NEWCOMB CARLTON, PRESIDENT

Check
Time Filed

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

via Galveston

JAN 19 1917

GERMAN LEGATION

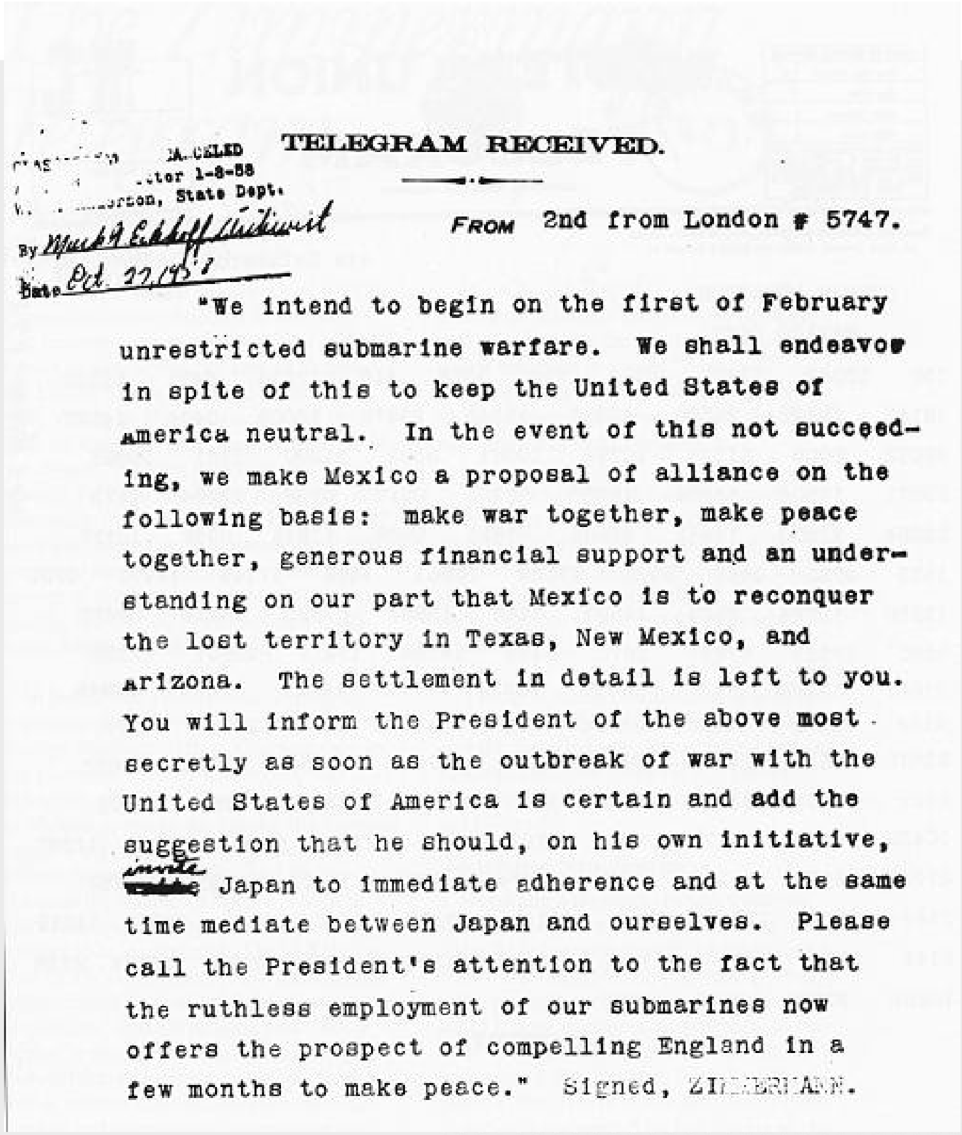
MEXICO CITY

```
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
```

BEPNSTOPFF.

Charge German Embassy.

Zimmerman Telegram cleartext



CA..CELED
..ctor 1-8-58
..erson, State Dept.
By Mark A. Eckhoff
Date Oct. 22, 1957

TELEGRAM RECEIVED.

FROM 2nd from London # 5747.

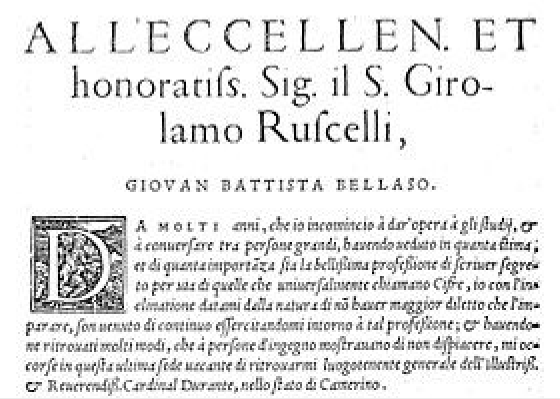
"We intend to begin on the first of February unrestricted submarine warfare. We shall endeavor in spite of this to keep the United States of America neutral. In the event of this not succeeding, we make Mexico a proposal of alliance on the following basis: make war together, make peace together, generous 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.

Book crypto

- Beale
- Three parts only part II is decrypted
- 115, 73, 24, 807, 37, 52, 49, 17, 31, 62, 647, 22, 7, 15, 140, 47, 29, 107, 79, 84, 56, 239, 10, 26, 811, 5, 196, 308, 85, 52, 160, 136, 59, 211, 36, 9, 46, 316, 554, 122, 106, 95, 53, 58, 2, 42, 7, 35, 122, 53, 31, 82, 77, 250, 196, 56, 96, 118, 71, 140, 287, 28, 353, 37, 1005, 65, 147, 807, 24, 3, 8, 12, 47, 43, 59, 807, 45, 316, 101, 41, 78, 154, 1005, 122, 138, 191, 16, 77, 49, 102, 57, 72, 34, 73, 85, 35, 371, 59, 196, 81, 92, 191, 106, 273, 60, 394, 620, 270, 220, 106, 388, 287, 63, 3, 6, 191, 122, 43, 234, 400, 106, 290, 314, 47, 48, 81, 96, 26, 115, 92, 158, 191, 110, 77, 85, 197, 46, 10, 113, 140, 353, 48, 120, 106, 2, 607, 61, 420, 811, 29, 125, 14, 20, 37, 105, 28, 248, 16, 159, 7, 35, 19, 301, 125, 110, 486, 287, 98, 117, 511, 62, 51, 220, 37, 113, 140, 807, 138, 540, 8, 44, 287, 388, 117, 18, 79, 344, 34, 20, 59, 511, 548, 107, 603, 220, 7, 66, 154, 41, 20, 50, 6,
- I have deposited in the county of Bedford about four miles from Bufords in an excavation or vault six feet below the surface of the ground the following articles belonging jointly to the parties whose names are given in number three herewith. The first deposit consisted of ten hundred and fourteen pounds of gold and thirty eight hundred and twelve pounds of silver deposited Nov eighteen nineteen. .....

Vigenère Cipher

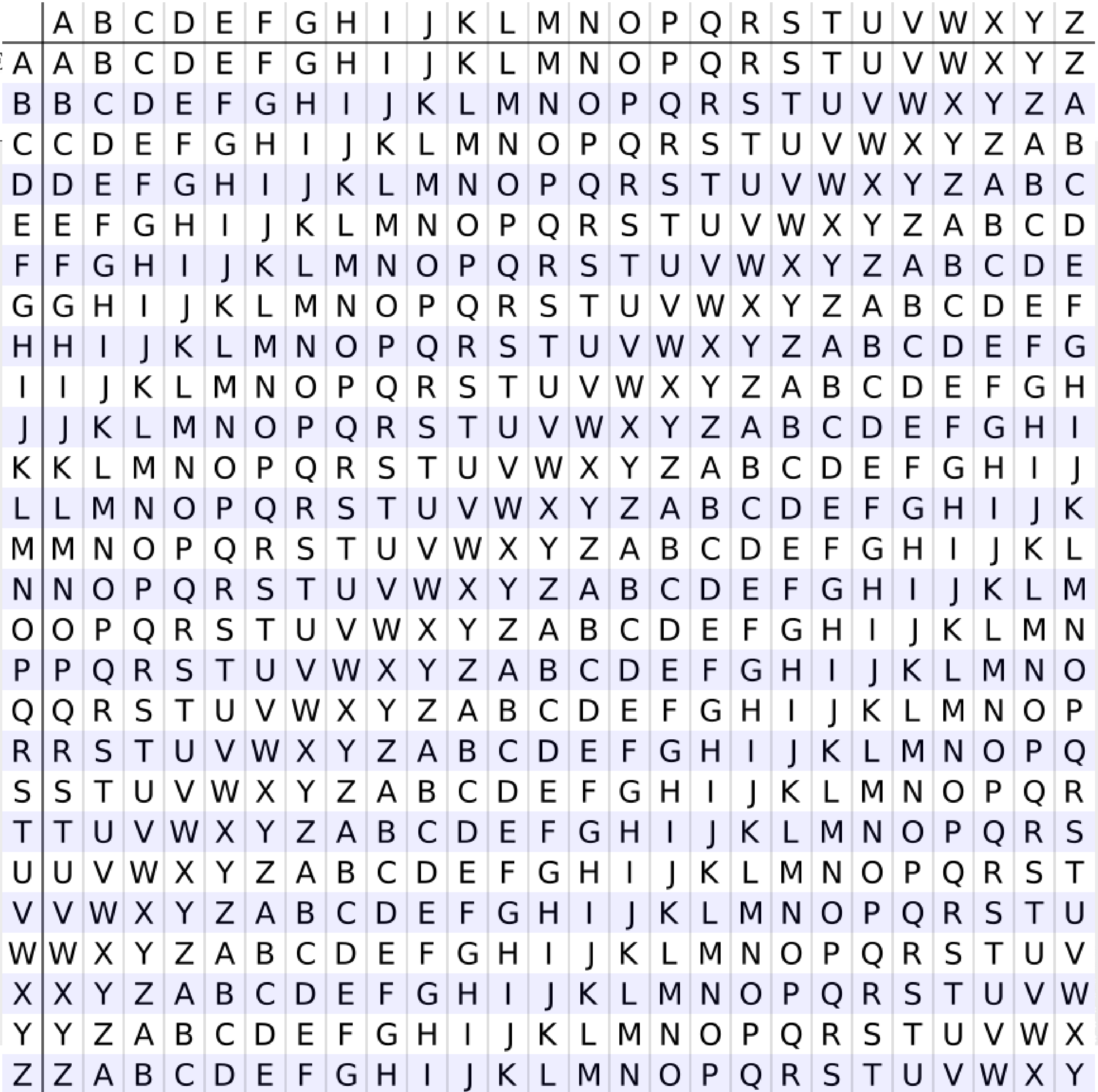
- Poly alphabetical cipher
- Reinvented over and over



ALL'ECCELLEN. ET honoratiſs. Sig. il S. Girolamo Ruſcelli,

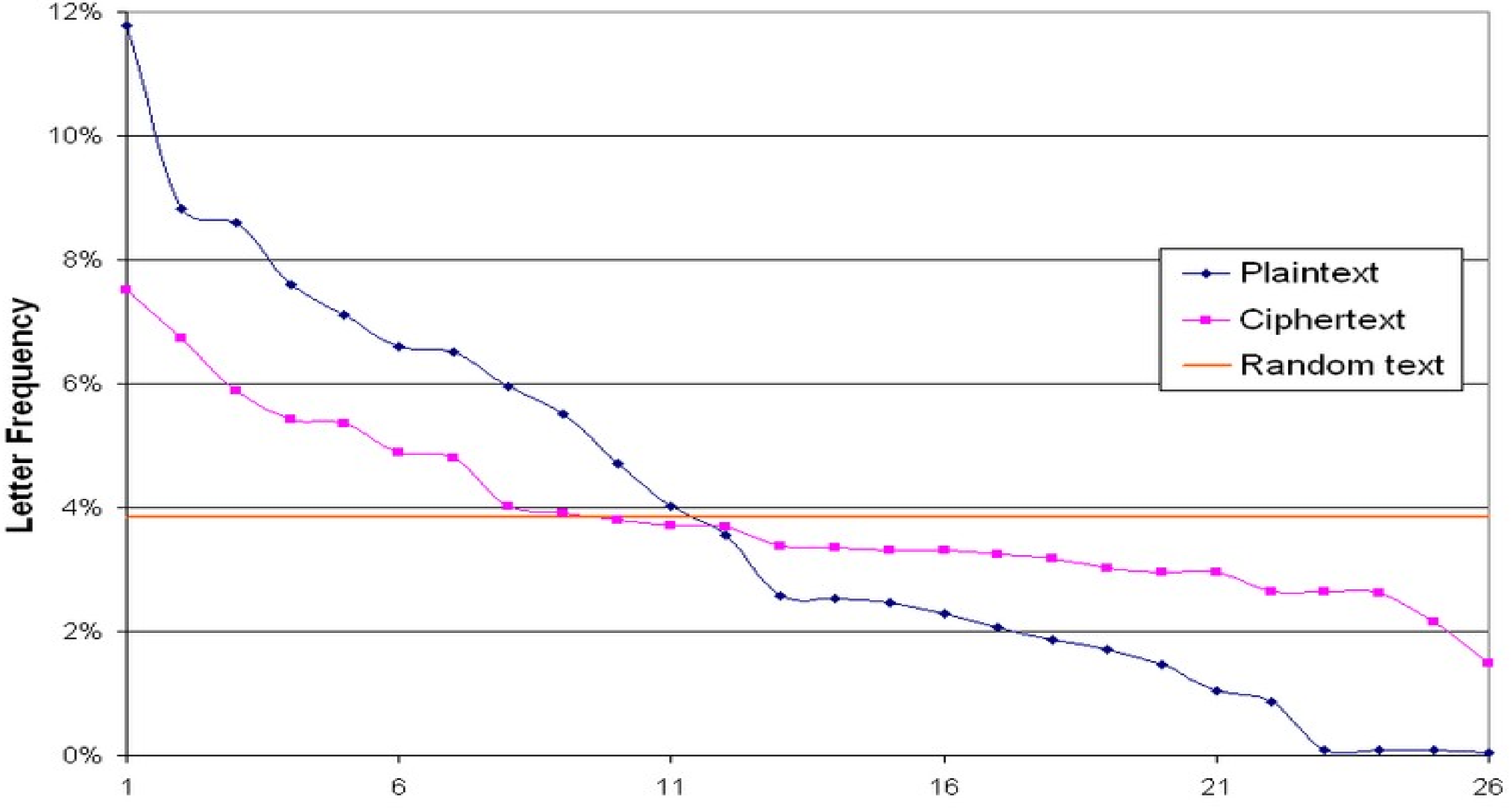
GIOVAN BATTISTA BELLASO.

DA MOLTI anni, che io incomincio à dar'opera à gli ſtudij, & à conuerſare tra perſone grandi, hauendo ueduto in quanta ſtima; et di quanta importãza ſia la belliſsima profeſsione di ſcriuer ſegreto per uia di quelle che uniuerſalmente chiamano Cifre, io con l'inclinatione datami dalla natura di nõ hauer maggior diletto che l'imparare, ſon uenuto di continuo eſſercitandomi intorno à tal profeſsione; & hauendone ritrouati molti modi, che à perſone d'ingegno moſtrauano di non diſpiacere, mi occorſe in queſta ultima ſede uacante di ritrouarmi luogotenente generale dell'illuſtriſs. & Reuerendiſs. Cardinal Durante, nello ſtato di Camerino.

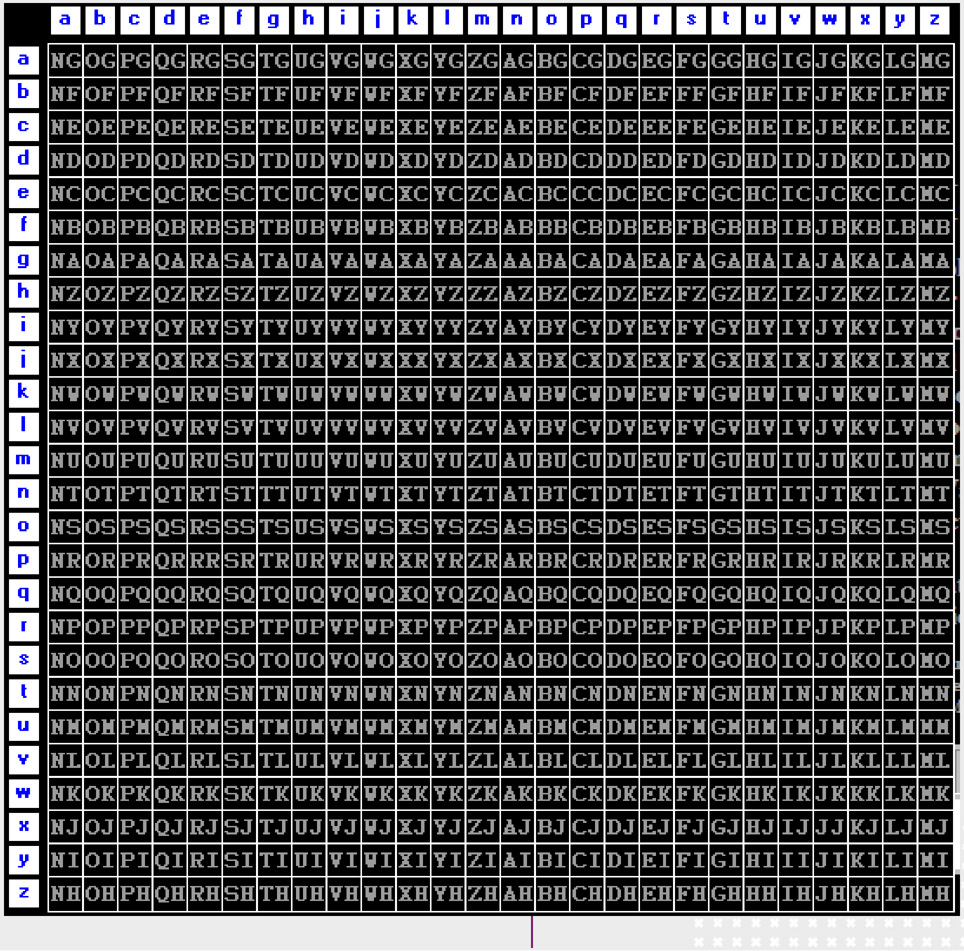


	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Frequency in Vigenère



Di-Graph table



	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
a	NG	OG	PG	QG	RG	SG	TG	UG	VG	WG	XG	YG	ZG	AG	BG	CG	DG	EG	FG	GG	HG	IG	JG	KG	LG	MG
b	NF	OF	PF	QF	RF	SF	TF	UF	VF	WF	XF	YF	ZF	AF	BF	CF	DF	EF	FF	GF	HF	IF	JF	KF	LF	MF
c	NE	OE	PE	QE	RE	SE	TE	UE	VE	WE	XE	YE	ZE	AE	BE	CE	DE	EE	FE	GE	HE	IE	JE	KE	LE	ME
d	ND	OD	PD	QD	RD	SD	TD	UD	VD	WD	XD	YD	ZD	AD	BD	CD	DD	ED	FD	GD	HD	ID	JD	KD	LD	MD
e	NC	OC	PC	QC	RC	SC	TC	UC	VC	WC	XC	YC	ZC	AC	BC	CC	DC	EC	FC	GC	HC	IC	JC	KC	LC	MC
f	NB	OB	PB	QB	RB	SB	TB	UB	VB	WB	XB	YB	ZB	AB	BB	CB	DB	EB	FB	GB	HB	IB	JB	KB	LB	MB
g	NA	OA	PA	QA	RA	SA	TA	UA	VA	WA	XA	YA	ZA	AA	BA	CA	DA	EA	FA	GA	HA	IA	JA	KA	LA	MA
h	NZ	OZ	PZ	QZ	RZ	SZ	TZ	UZ	VZ	WZ	XZ	YZ	ZZ	AZ	BZ	CZ	DZ	EZ	FZ	GZ	HZ	IZ	JZ	KZ	LZ	MZ
i	NY	OY	PY	QY	RY	SY	TY	UY	VY	WY	XY	YY	ZY	AY	BY	CY	DY	EY	FY	GY	HY	IY	JY	KY	LY	MY
j	NX	OX	PX	QX	RX	SX	TX	UX	VX	WX	XX	YX	ZX	AX	BX	CX	DX	EX	FX	GX	HX	IX	JX	KX	LX	MX
k	NW	OW	PW	QW	RW	SW	TW	UW	VW	WW	XW	YW	ZW	AW	BW	CW	DW	EW	FW	GW	HW	IW	JW	KW	LW	MW
l	NV	OV	PV	QV	RV	SV	TV	UV	VV	WV	XV	YV	ZV	AV	BV	CV	DV	EV	FV	GV	HV	IV	JV	KV	LV	MV
m	NU	OU	PU	QU	RU	SU	TU	UU	VU	WU	XU	YU	ZU	AU	BU	CU	DU	EU	FU	GU	HU	IU	JU	KU	LU	MU
n	NT	OT	PT	QT	RT	ST	TT	UT	VT	WT	XT	YT	ZT	AT	BT	CT	DT	ET	FT	GT	HT	IT	JT	KT	LT	MT
o	NS	OS	PS	QS	RS	SS	TS	US	VS	WS	XS	YS	ZS	AS	BS	CS	DS	ES	FS	GS	HS	IS	JS	KS	LS	MS
p	NR	OR	PR	QR	RR	SR	TR	UR	VR	WR	XR	YR	ZR	AR	BR	CR	DR	ER	FR	GR	HR	IR	JR	KR	LR	MR
q	NQ	OQ	PQ	QQ	RQ	SQ	TQ	UQ	VQ	WQ	XQ	YQ	ZQ	AQ	BQ	CQ	DQ	EQ	FQ	GQ	HQ	IQ	JQ	KQ	LQ	MQ
r	NP	OP	PP	QP	RP	SP	TP	UP	VP	WP	XP	YP	ZP	AP	BP	CP	DP	EP	FP	GP	HP	IP	JP	KP	LP	MP
s	NO	OO	PO	QO	RO	SO	TO	UO	VO	WO	XO	YO	ZO	AO	BO	CO	DO	EO	FO	GO	HO	IO	JO	KO	LO	MO
t	NN	ON	PN	QN	RN	SN	TN	UN	VN	WN	XN	YN	ZN	AN	BN	CN	DN	EN	FN	GN	HN	IN	JN	KN	LN	MN
u	NM	OM	PM	QM	RM	SM	TM	UM	VM	WM	XM	YM	ZM	AM	BM	CM	DM	EM	FM	GM	HM	IM	JM	KM	LM	MM
v	NL	OL	PL	QL	RL	SL	TL	UL	VL	WL	XL	YL	ZL	AL	BL	CL	DL	EL	FL	GL	HL	IL	JL	KL	LL	ML
w	NK	OK	PK	QK	RK	SK	TK	UK	VK	WK	XK	YK	ZK	AK	BK	CK	DK	EK	FK	GK	HK	IK	JK	KK	LK	MK
x	NJ	OJ	PJ	QJ	RJ	SJ	TJ	UJ	VJ	WJ	XJ	YJ	ZJ	AJ	BJ	CJ	DJ	EJ	FJ	GJ	HJ	IJ	JJ	KJ	LJ	MJ
y	NI	OI	PI	QI	RI	SI	TI	UI	VI	WI	XI	YI	ZI	AI	BI	CI	DI	EI	FI	GI	HI	II	JI	KI	LI	MI
z	NH	OH	PH	QH	RH	SH	TH	UH	VH	WH	XH	YH	ZH	AH	BH	CH	DH	EH	FH	GH	HH	IH	JH	KH	LH	MH

Polyalphabetical substitution

```
VNRARPBHPAHWTRVFFXWVRKBQWGMERWCASOAEKQNTOSJASUGSTRVAFEFNQWEMUNRYRVENRENXZRQSGMUVEFPVQCX
GYSYVWLNRVPSECYLRVKPMWAXAFXZRMKNZAFMLVRYCVGSIKFSJNXUNWSNXJHLJHRAIIJFMLLFGPLMZEKJIDYEKNVWFISEGZ
CVGSIKFSJBJUBQHHXWEWUVIFPISGXZRYFVZWEWAGCGSMDYMFBMKNXUUMUNKGOIXBVWGLAFLWJEKNTJBJWFWGETWEW
GBRDVNCUSGTPWEESEMFGLWQIHNVLZIFGSXZELUIENXAPWSAHUBQHHXWEWUVIFPISGXZRIAAHZBZWAYFVZWEWAGCGSX
WPLFBPGTCUVXSGMGARWRHWQISEPQYMXRFWERKGIAAELGIFQIVOIDYTGEXZVKZFGZBSDNTMOPAPLATLKPLGBPGAPGAKA
FPSAHYEEVHELVRYVRSGXZREYRSXGLWFEERCWNVZRVSAOWQJASXZVRLUIORWLVRYUSMFIKPMWAGWGEDRRLFISEGZVRS
GXZREYRSXUISPLARZWQELBTJNRCVRYVRLUIOVPDVEEYSORPDCYLAEEZELUIENXAPEDPSECILVXABRTRVFFXWVRWNVFRHS
OEAAQSGLWZELVGKSVGZRWJCGEOMAMNRVKVXQNRVNTZQMFZELUIENXAPWXESEGLWHRAIIJFMLLSXPEDVJGERANFWEOW
YIQJLWEIZRWLHHARHMAHWELWAHJVODRRKGVSPMLNXABRFRIVRHTRVFFXWVRNHRAGIVFXSGIKGLWRBHBVLBJUECHGSYE
EHUCXESEGLWHRAGIVFXSGIKJEKPSFGVGYPWQEKNQMAMLVSFFXSEXAAKXESEGLWPSDQASEYFGMDEIUNXWTSJVDSGMGA
MFJMLUJMEXZRVJRPSKELVSFVRLUIDNXWFMFOIJAWLRMFOVGHKZGXZRGGHVLPEKRFWERKGIAAZMAMLRHKGELRWLUIJHPA
AKAAXZRGSFIVRGDNVWQXZNXKBJLJEJRASFTJBXWPXWQWHRIUUYFQIJGLWSMJFXSZIFQQWAXOUMUUGGAXJVFMGIVGSJRK
MYELBVQPLSAKWFVWQYUVRYPSFGVGYWGAIFPVQCXABRTRVFFXWVRONWGEMYVRSYPQEIHEIKRRLRHTLXZRIDRGLESFVGX
ESFGMWEJGHRVNXABRZRPSGIJEIHEIKRRLRHZVQKRPXPVQCXGTVSCLQOIJAWLRMFQIKVKFRHLUIKNPKNWLEISZGACLWEMF
NRVFYTZMLGIVVXLBIKGVWNQXBVJRZARASAHHBWKVFDRWLNRVNVVVDSGMGALWYELRVHHFDVWZRHLUIUUEUUENNVANRL
BJKNPKNMFVRZRTJBTGFIVGLWRPDVTLVGUHVNRGMEZWNWSOEKVWXBVHHFDVGCRCKPLWZIKUIOBVCRHSFXZRPWNHJRW
WNVUUIJBRLUIWQZWEWABRGSIVQWSGLWNPYBVAGLEFQSQILUIAEASLMFGSHBTMYEJFSXGASEIXBVWKEECPWFMFPIOUIFB
TWAWKUMKPSECMDRHOVXZBYLBTWAWKYXZRCHBAWEQGFXGSMLFSHRVSGMGAWSAHGCIFOWVCEUXEYRWATRAAKAFFSFI
VBRWQRWNVDLEVRGSQIDNXWEIVJEJQWFBAVRRVVWUYSKRHENWKFYJIIAYPSAGWOCLUIFNXABRSYWWPYJVXQNKWAGQNR
VEIKREJPLWEWVVWUBZWEIVNFSPOVBSJVRLUISTIFPCKQYSYIUQVTTEDTSJVXZZXZRWWRZWAXKEEAFIVFYKCMUVSFFSXGL
WRPDVTLVGUHVNRTSEEERXWEWHESHBWWQFQAWSNRVFXSAHSEHAMIVOCFVWLZEFLVWFISEGZRVKSISEIVGLSGXZRRKNL
SQGZBWWAGMEZWFXZNXYNZWGLWZEUECHGEFNPQGMUNHNNRLNKWTSGTPWFIDRGLRHUUEUUESYSFTAAGLTRVFFXWVR
KCSDLQWFWSTISHXZRRLVGSGMGAGGQIXBVMFIAAXDFAZVGZVWOVHWYCMFIVSSJVRLRVFRXKRGMEMLLQSACHESLBGGYW
TNWWQSFUMKJSJXWZNZWOIWAEVBTLRHTLZSEMGHWKGEFQEJQWGEKSAMRNXABRKNRVNVWHWWQMFNZSEMWGCGSEHC
PAPELVSFFWMPLSFEHCPWVSKGLWYMFHBCRVFRPGCIFFWZNRVGSJVRKCVAAKTRVFFXWVRLNYYUXSPSMEWWBRZVKZFTW
RHUECHGSYEEHUCZRMFGVGQYURHFRAUNGZRELGEUXWSTEAAWLVQHYIERRLNXABRKBJSRWAAXZRWSZILVQWCIJVSVVRS
CVAYFWERKGIAAWKGVWNQUVTZRVKNPKNASFWWYIUGIVNWSZIEOIJBJLUIXVRSYTGEXXBPABSXGLWRWLEISZTJBNWPXHNV
LBJSRYJBTWNRMAMGAVWFISEGZQMJRGLVZWVRTRVFFXWVRHHFDVWZRHJSWTNZSEMSAXGSXZRJSFXKLRVESERFSFIVUEK
UJMAGLVSFUIAFSFRSXGLWRHAGSJFSXGLWOSGXTGFXIHEFGYEPVQCXGTVSCLQ
```

One-Time Pad: Encryption

e=000 h=001 i=010 k=011 l=100 r=101 s=110 t=111

Encryption: Plaintext ⊕ Key = Ciphertext

	h	e	i	l	h	i	t	l	e	r
Plaintext:	001	000	010	100	001	010	111	100	000	101
Key:	111	101	110	101	111	100	000	101	110	000
Ciphertext:	110	101	100	001	110	110	111	001	110	101
	s	r	l	h	s	s	t	h	s	r

One-Time Pad: Decryption

e=000 h=001 i=010 k=011 l=100 r=101 s=110 t=111

Decryption: Ciphertext ⊕ Key = Plaintext

	s	r	l	h	s	s	t	h	s	r
Ciphertext:	110	101	100	001	110	110	111	001	110	101
Key:	111	101	110	101	111	100	000	101	110	000
Plaintext:	001	000	010	100	001	010	111	100	000	101
	h	e	i	l	h	i	t	l	e	r

One-Time Pad

Double agent claims sender used following “**key**”

	s	r	l	h	s	s	t	h	s	r
Ciphertext:	110	101	100	001	110	110	111	001	110	101
“**key**”:	101	111	000	101	111	100	000	101	110	000
“Plaintext”:	011	010	100	100	001	010	111	100	000	101
	k	i	l	l	h	i	t	l	e	r

e=000 h=001 i=010 k=011 l=100 r=101 s=110 t=111

One-Time Pad

Double agent claims sender used following “**key**”

	s	r	l	h	s	s	t	h	s	r
Ciphertext:	110	101	100	001	110	110	111	001	110	101
“**key**”:	101	111	000	101	111	100	000	101	110	000
“Plaintext”:	011	010	100	100	001	010	111	100	000	101
	k	i	l	l	h	i	t	l	e	r

e=000 h=001 i=010 k=011 l=100 r=101 s=110 t=111

One-Time Pad Summary

- **Provably** secure…
  - Ciphertext provides **no** info about plaintext
  - All plaintexts are equally likely
- …but, only when used correctly
  - Pad must be random, used only once
  - Pad is known only to sender and receiver
- Note: pad (key) is same size as message

Real-World One-Time Pad

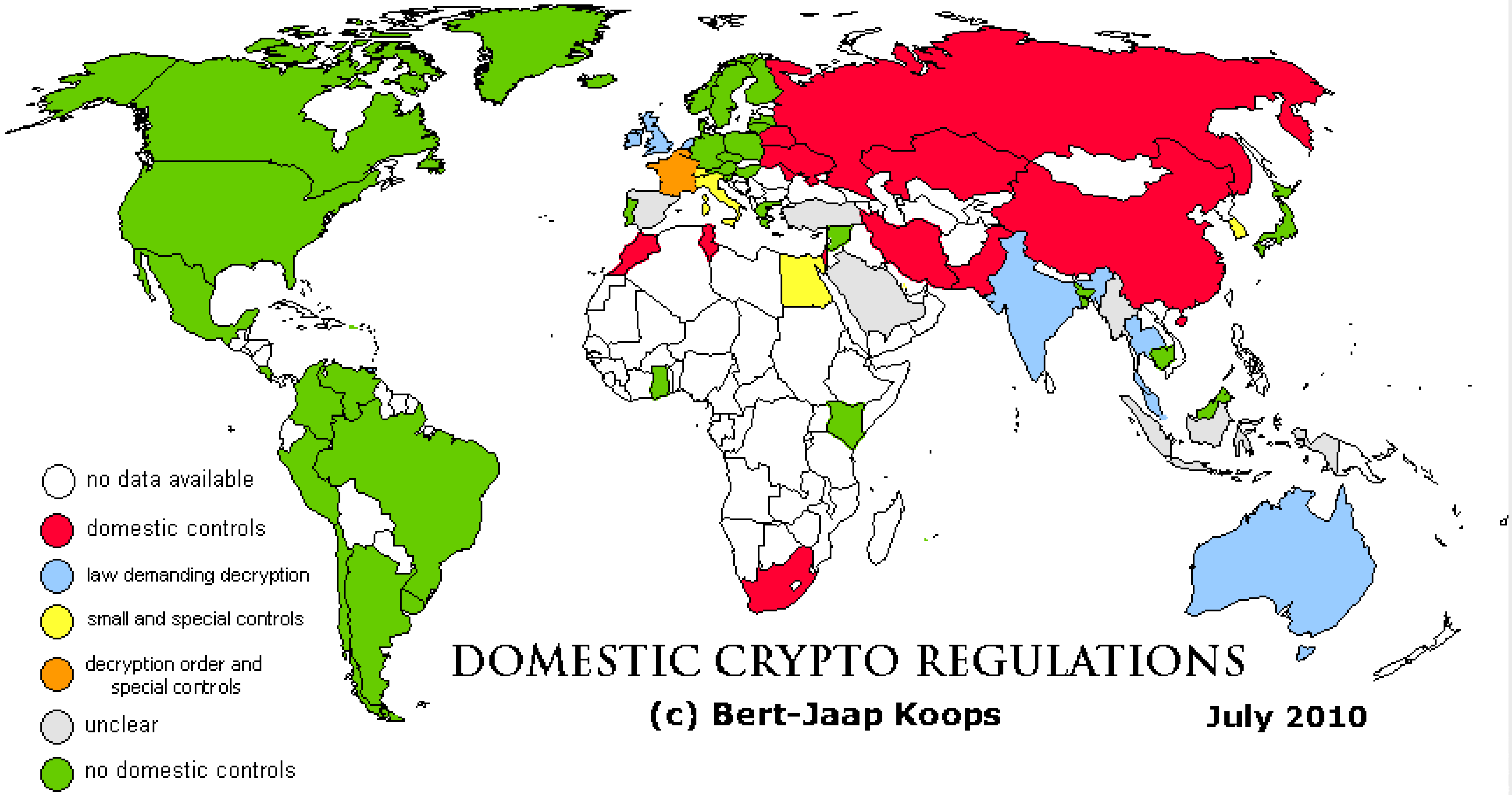
- Project VENONA
  - Encrypted spy messages from U.S. to Moscow in 30’s, 40’s, and 50’s
  - Nuclear espionage, etc.
  - Thousands of messages
- Spy carried one-time pad into U.S.
- Spy used pad to encrypt secret messages
- Repeats within the “one-time” pads made cryptanalysis possible

Crypto Law

- Import controls
- Export controls
- Domestic Controls
- Wassenaar Arrangement
- Overview Bert Jaap Koops:

http://rechten.uvt.nl/koops/cryptolaw/

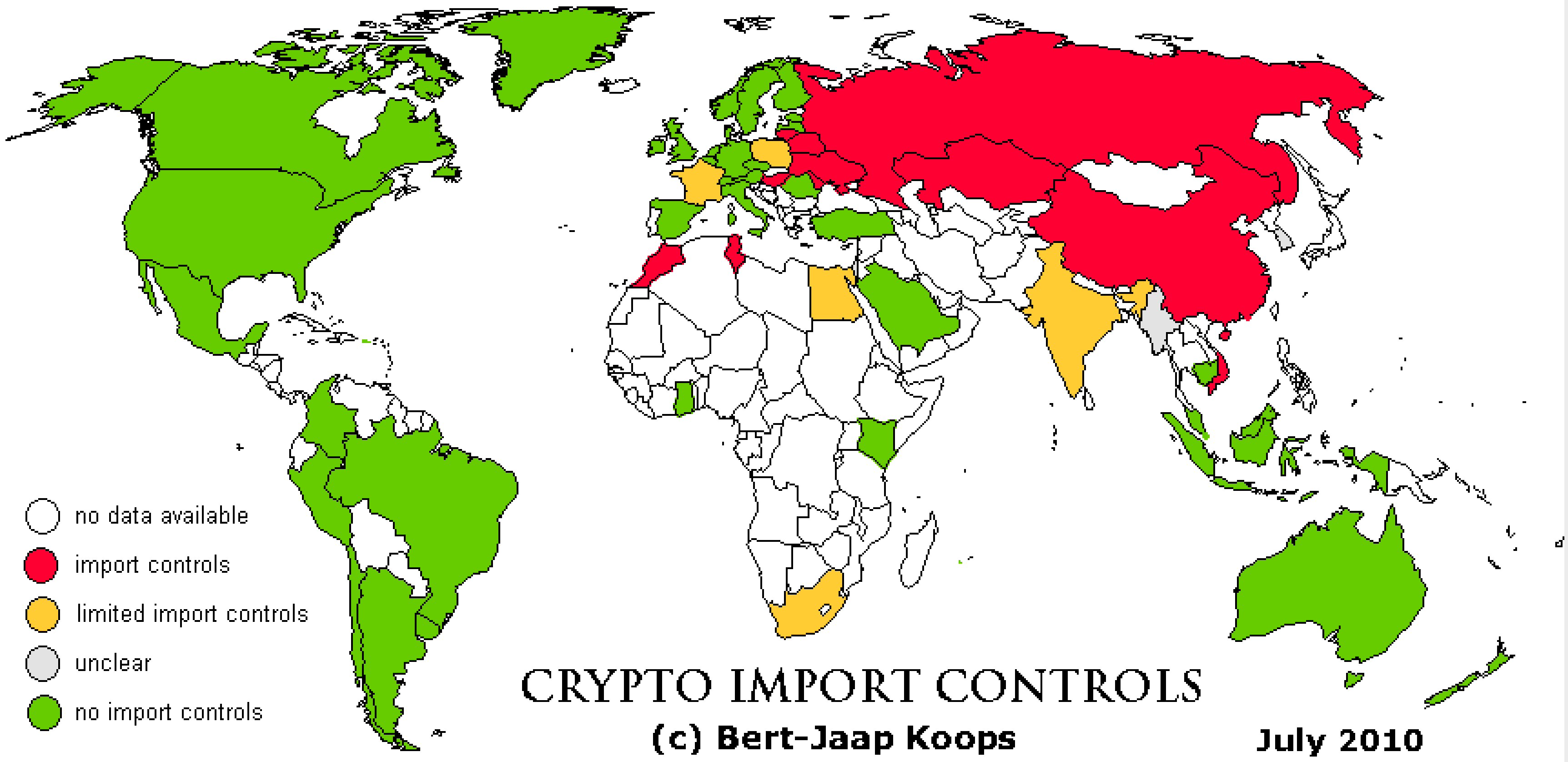
Crypto Law


○ no data available
🔴 domestic controls
🔵 law demanding decryption
🟡 small and special controls
🟠 decryption order and special controls
⚪ unclear
🟢 no domestic controls

DOMESTIC CRYPTO REGULATIONS

(c) Bert-Jaap Koops July 2010

Crypto Law

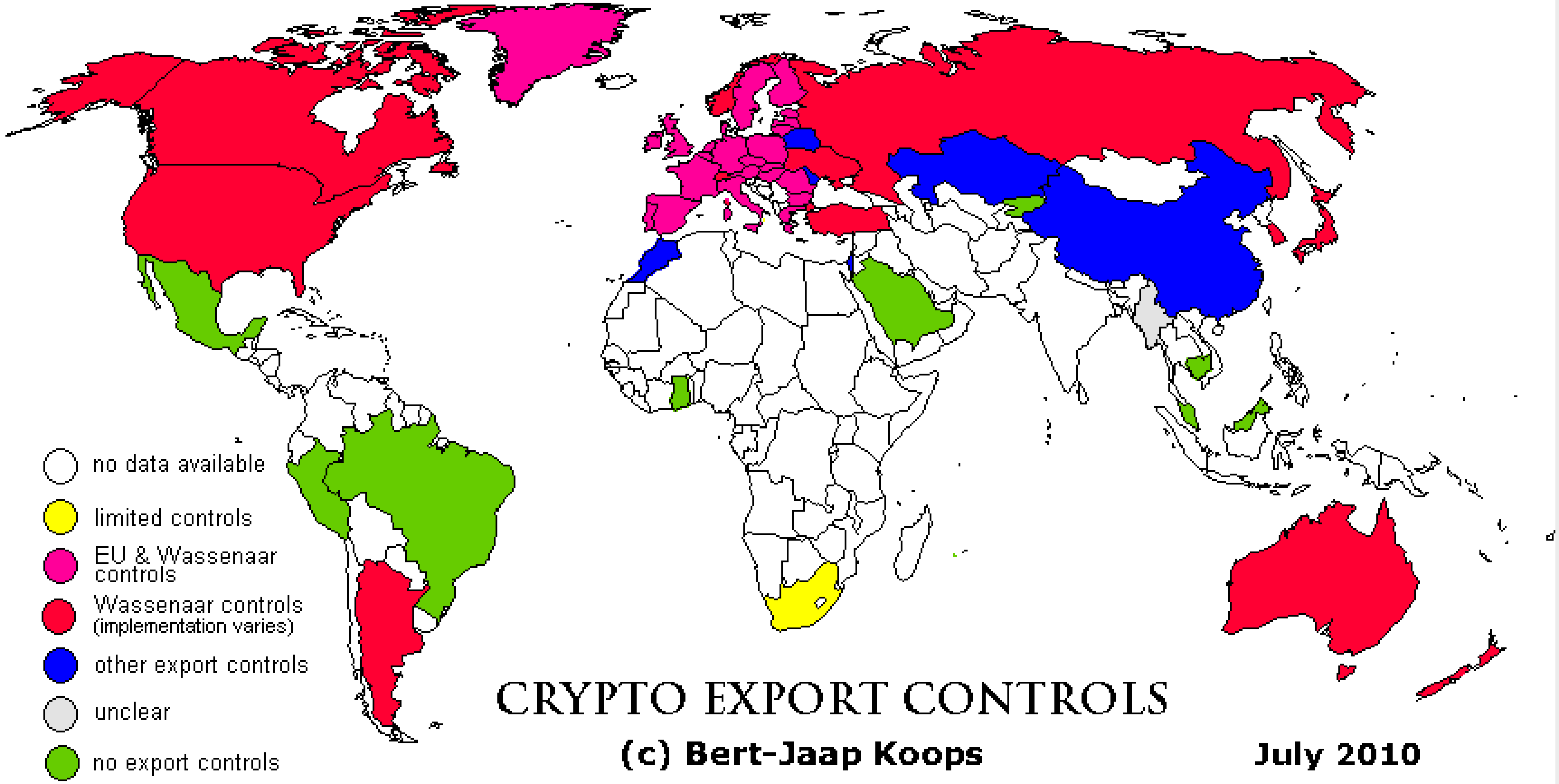


CRYPTO IMPORT CONTROLS

(c) Bert-Jaap Koops

July 2010

Crypto Law



CRYPTO EXPORT CONTROLS

(c) Bert-Jaap Koops

July 2010