Κρυπτογραφία

Καθηγητής Π. Λουρίδας

Τμήμα Διοικητικής Επιστήμης και Τεχνολογίας,
Οικονομικό Πανεπιστήμιο Αθηνών
louridas@aueb.gr

Επισκόπηση

Επισκόπηση

- Αρχικό κείμενο (plaintext) είναι το κείμενο που θέλουμε να στείλουμε στον παραλήπτη.
- Κρυπτογραφημένο κείμενο (ciphertext) είναι το κείμενο που θέλουμε να στείλουμε στον παραλήπτη, ώστε μόνο αυτός να μπορεί να το καταλάβει.
- Κρυπτογράφηση είναι η μετατροπή του αρχικού κειμένου σε κρυπτογραφημένο κείμενο.
- Αποκρυπτογράφηση είναι η επαναφορά του κρυπτογραφημένου κειμένου στο αρχικό κείμενο.
- Η κρυπτογράφιση και η αποκρυπτογράφηση βασίζονται στη χρήση ενός κλειδιού (key).

Επισκόπηση

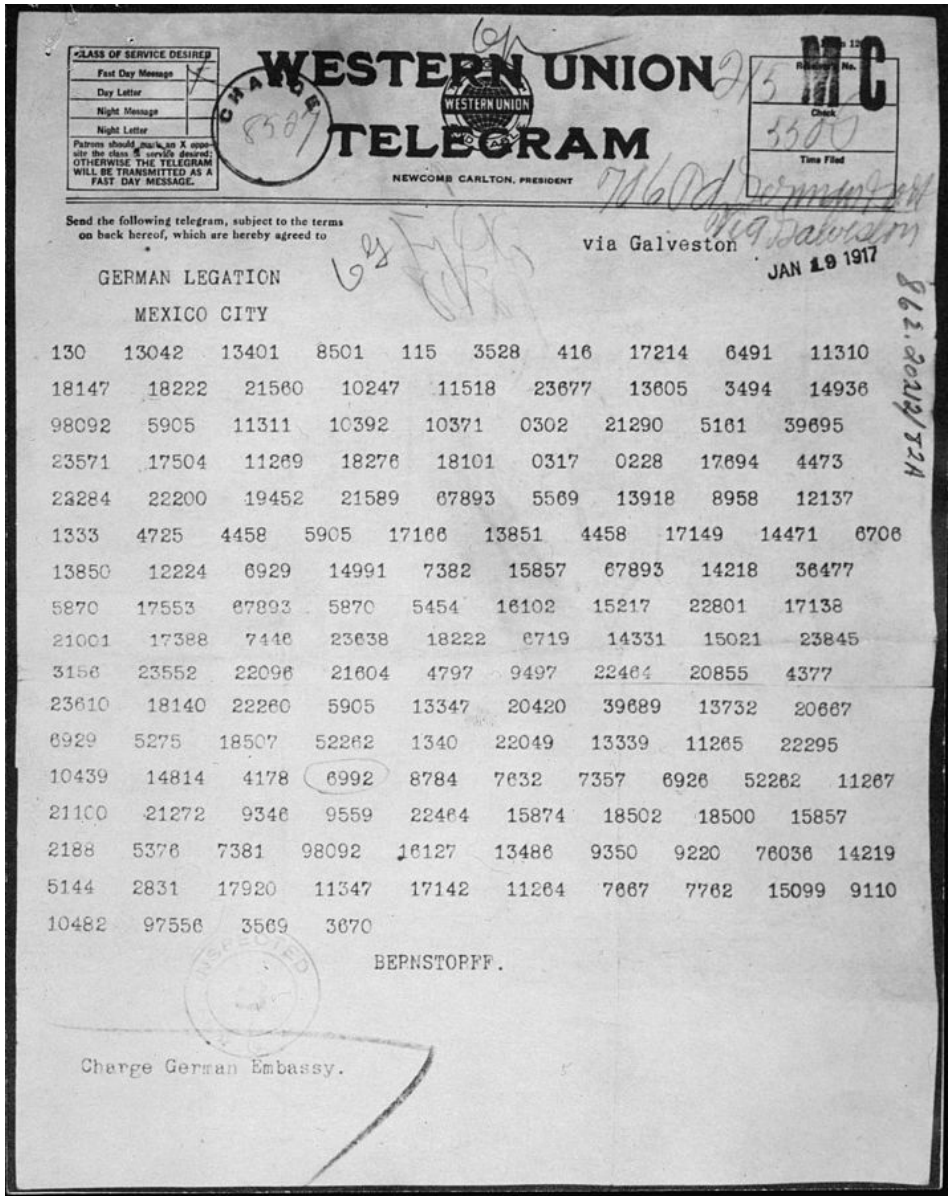
Κρυπτογραφία στην Αρχαιότητα

- Μία από τις πρώτες μεθόδους κρυπτογράφησης ήταν η Σπαρτιατική Σκυτάλη.
- Στη Ρωμαϊκή εποχή χρησιμοποιήθηκαν συστήματα αντικατάστασης γραμμάτων (substitution ciphers).

Σπαρτιατική Σκυτάλη

https://en.wikipedia.org/wiki/Scytale

Τηλεγράφημα Zimmermann



WESTERN UNION TELEGRAM

NEWCOMB CARLTON, PRESIDENT

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.

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.

https://en.wikipedia.org/wiki/Zimmermann_Telegram

Σύστημα Κρυπτογράφησης Καίσαρα (Caesar Substitution Cipher)

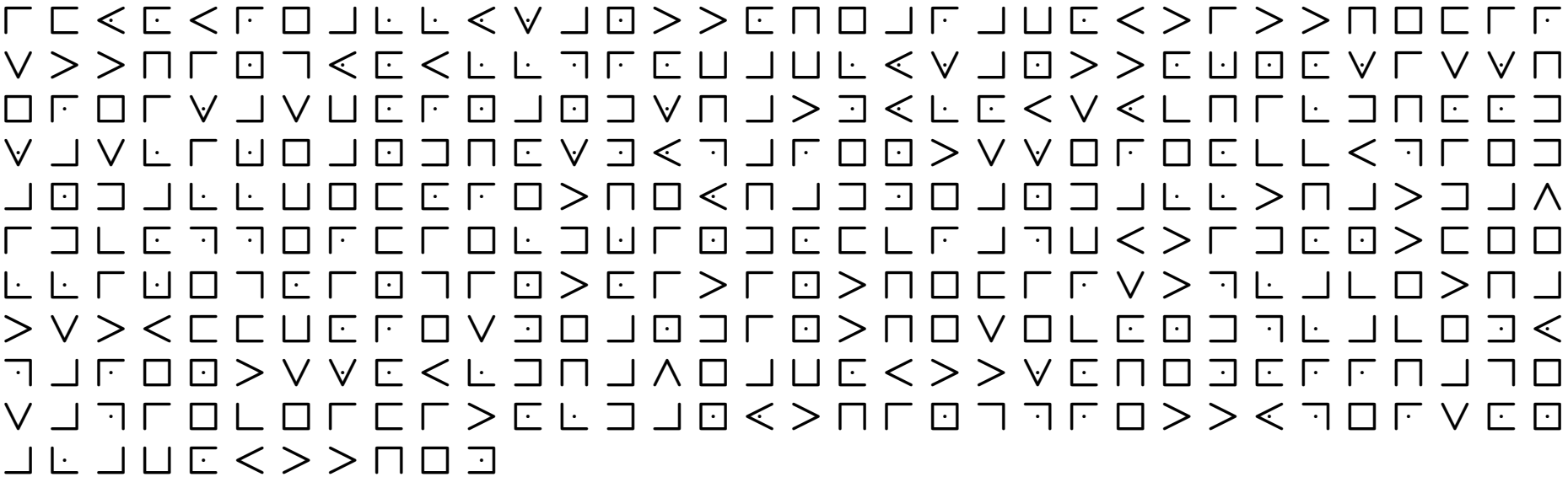
- Αντικαθιστούμε κάθε γράμμα με ένα άλλο, που βρίσκεται συγκεκριμένο αριθμό θέσεων στο αλφάβητο μετά από το πρώτο.
- Ο αριθμός θέσεων που μετακινούμαστε είναι το κλειδί της κρυπτογράφησης.
- Με κλειδί 5, το A γίνεται F, το B γίνεται G, ..., μέχρι το Z που γίνεται E.

Παράδειγμα Κρυπτογράφησης Καίσαρα

- Έστω ότι έχουμε τη φράση “I am seated in an office”.
- Αυτή, με κλειδί 5, κωδικοποιείται ως: N FR XJFYJI NS FS TKKNHJ.
- Για την αποκωδικοποίηση αρκεί να κάνουμε το ίδιο, αλλάζοντας κάθε γράμμα όμως με το γράμμα που προηγείται 5 θέσεις στο αλφάβητο.

Επισκόπηση

Το Μήνυμα



Συχνότητες Αγγλικών Γραμμάτων

- Το 1965 ο Mark Mayzner δημοσίευσε πίνακες συχνοτήτων της αγγλικής γλώσσας.
- Με την τεχνολογία της εποχής μπορέσε να χρησιμοποιήσει ένα σώμα κειμένων (corpus) μεγέθους 20.000 λέξεων.
- Στις 17 Δεκεμβρίου 2012 επικοινώνησε με τον Peter Norvig, Διευθυντή Έρευνας στη Google, ρωτώντας αν η Google θα μπορούσε να χρησιμοποιήσει τους πόρους της για την ενημέρωση των πινάκων που είχε φτιάξει.
- Ο Norvig το έκανε, και δημοσίευσε τα αποτελέσματα στο `http://norvig.com/mayzner.html`.

Πίνακας Συχνοτήτων

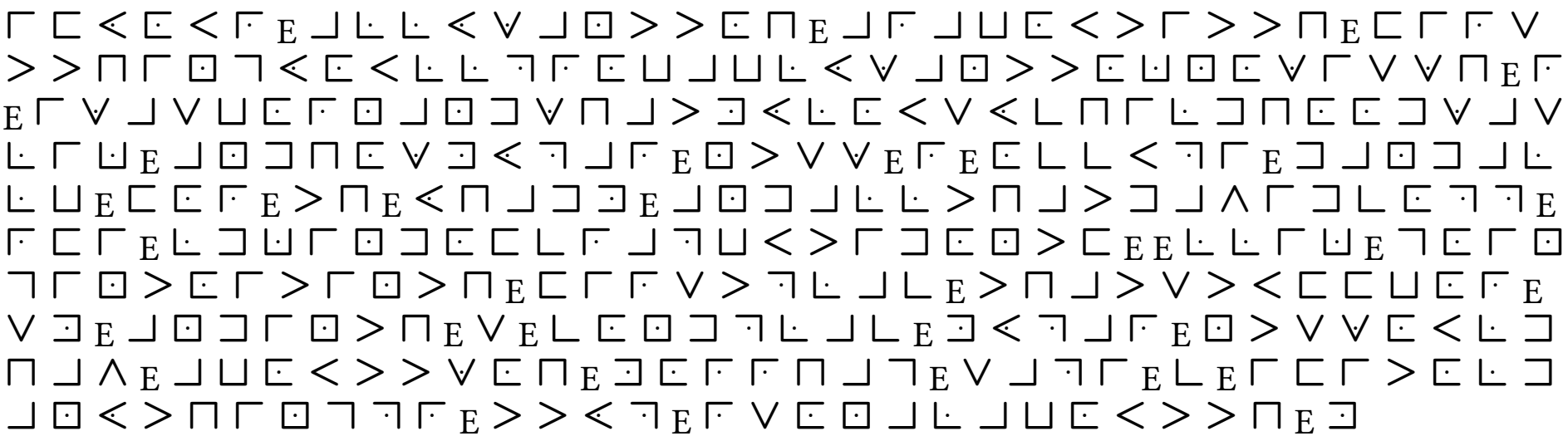
E	445,2	12,49%	M	89,5	2,51%
T	330,5	9,28%	F	85,6	2,40%
A	286,5	8,04%	P	76,1	2,14%
O	272,3	7,64%	G	66,6	1,87%
I	269,7	7,57%	W	59,7	1,68%
N	257,8	7,23%	Y	59,3	1,66%
S	232,1	6,51%	B	52,9	1,48%
R	223,8	6,28%	V	37,5	1,05%
H	180,1	5,05%	K	19,3	0,54%
L	145,0	4,07%	X	8,4	0,23%
D	136,0	3,82%	J	5,7	0,16%
C	119,2	3,34%	Q	4,3	0,12%
U	97,3	2,73%	Z	3,2	0,09%

Καταμετρήθηκαν 3.563.505.777.820 γράμματα. Οι αριθμοί αντιστοιχούν σε δισεκατομμύρια, και τα σχετικά ποσοστά εμφάνισής τους.

Αποκρυπτογράφηση του Μηνύματος

- Μετρούμε τις συχνότητες των συμβόλων στο κρυπτογραφημένο μήνυμα.
- Το πιο κοινό σύμβολο είναι το □ με 35 εμφανίσεις.
- Στη συνέχεια έχουμε το σύμβολο > με 33 εμφανίσεις.
- Τρίτο είναι το σύμβολο ⌟ με 32 εμφανίσεις.

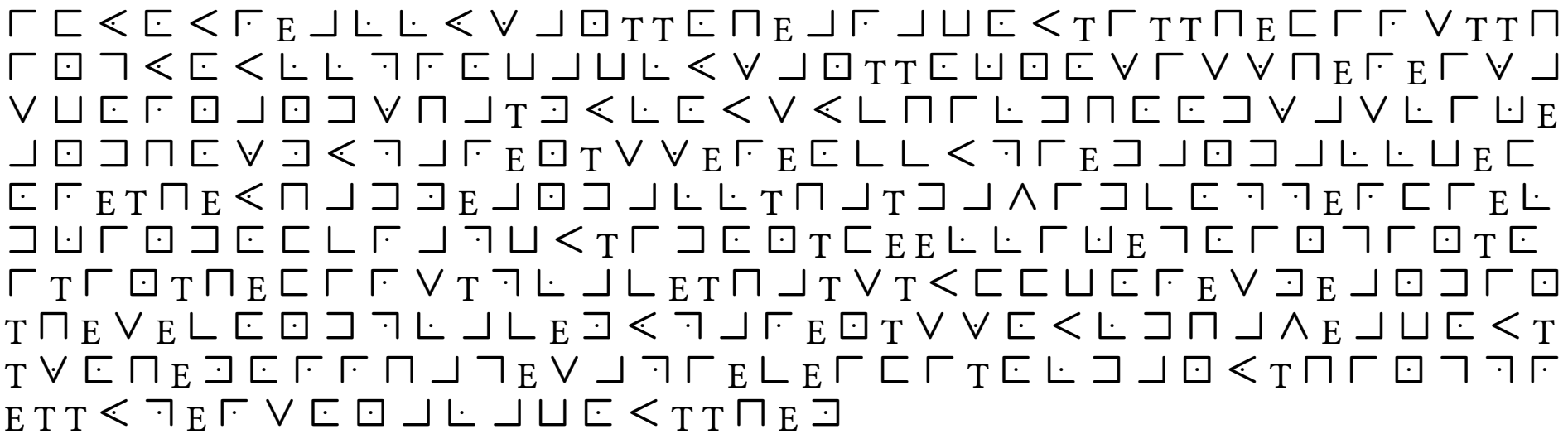
Αντικατάσταση του □ → E



Αντικατάσταση

□ → E

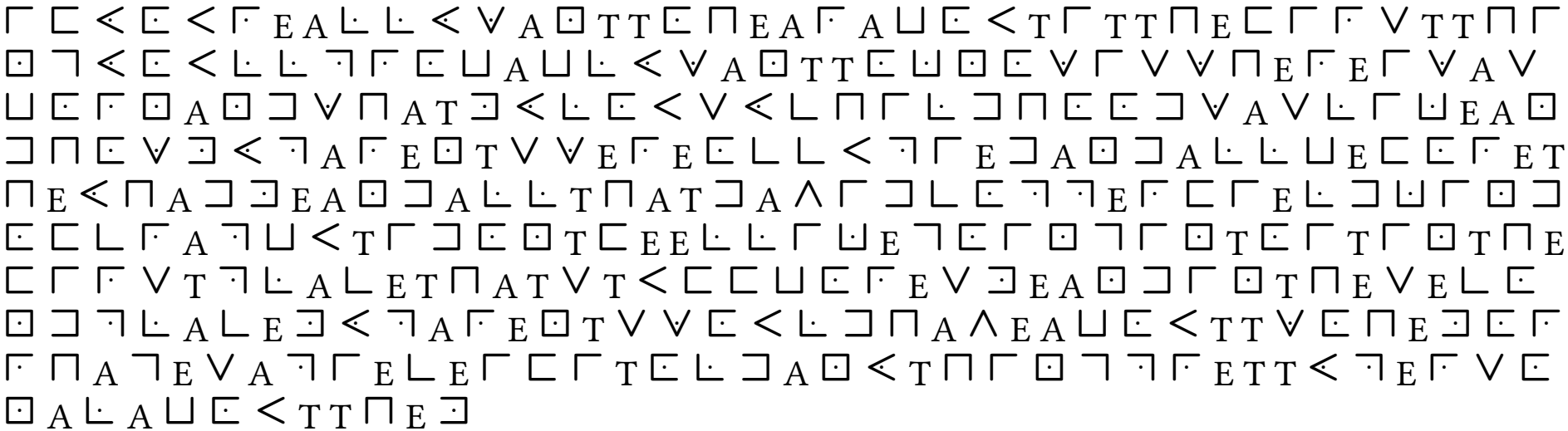
Αντικατάσταση > → T



Αντικατάσταση

> → T

Αντικατάσταση ⌟ → A



Αντικατάσταση

⌟ → A

Αποκρυπτογράφηση του Μηνύματος (2)

- Το σύμβολο $\sqsubset\!\!\cdot$ έχει 28 εμφανίσεις.
- Το σύμβολο $\ulcorner$ έχει 24 εμφανίσεις.
- Το σύμβολο $\boxdot$ έχει 22 εμφανίσεις.

Αντικατάσταση των ⊏· → Ο, ⌜· → Ι, ⊡ → Ν

Ι⊏ <· Ο < ⌜· ΕΑ└· └· <· ∨· ΑΝΤΤΟ⊓ΕΑ⌜· Α⊔Ο < ΤΙΤΤ⊓Ε⊏Ι⌜· ∨ ΤΤ⊓ΙΝ¬ <·
Ο < └· └· ¬⌜· Ο⊔Α⊔└· <· ∨· ΑΝΤΤΟ⊔ΝΟ∨ Ι∨ ∨·⊓Ε⌜· ΕΙ∨ Α∨⊔Ο⌜· ΝΑΝ⊐
∨·⊓ΑΤ⊐ <· └· Ο < ∨ <· └ ⊓Ι└· ⊐⊓ΟΟ⊐∨ Α∨└· Ι⊔ΕΑΝ⊐⊓Ο∨ ⊐ <· ¬Α⌜· Ε
ΝΤ∨ ∨·Ε⌜· ΕΟ└ └ < ¬ΙΕ⊐ΑΝ⊐Α└· └· ⊔Ε⊏Ο⌜· ΕΤ⊓Ε <·⊓Α⊐ ⊐ΕΑΝ⊐Α└·
└· Τ⊓ΑΤ⊐Α∧Ι⊐└Ο ¬· ¬·Ε⌜· ⊏ΙΕ└· ⊐⊔ΙΝ⊐Ο⊏└⌜· Α ¬·⊔ <·ΤΙ⊐ΟΝΤ⊏Ε
Ε└· └· Ι⊔Ε ¬ΟΙΝ ¬ΙΝΤΟΙΤΙΝΤ⊓Ε⊏Ι⌜· ∨ Τ ¬· └· Α└ΕΤ⊓ΑΤ∨ Τ <⊏⊏⊔Ο
⌜· Ε∨ ⊐ΕΑΝ⊐ΙΝΤ⊓Ε∨Ε└ΟΝ⊐ ¬· └· Α└Ε⊐ < ¬Α⌜· ΕΝΤ∨ ∨·Ο <· └· ⊐⊓Α
∧ΕΑ⊔Ο <· ΤΤ∨·Ο⊓Ε⊐Ο⌜· ⌜· ⊓Α ¬Ε∨Α ¬·ΙΕ└ ΕΙ⊏ΙΤΟ└· ⊐ΑΝ <·Τ⊓ΙΝ¬
¬·⌜· ΕΤΤ <· ¬·Ε⌜· ∨ ΟΝΑ└· Α⊔Ο <· ΤΤ⊓Ε⊐

Αντικατάσταση

⊏· → Ο, ⌜· → Ι, ⊡ → Ν

Συχνότητες Αγγλικών Διγραμμάτων

TH	100,3	3,56%
HE	86,7	3,07%
IN	68,6	2,43%
ER	57,8	2,05%
AN	56,0	1,99%
RE	52,3	1,85%
ON	49,6	1,76%
AT	41,9	1,49%
EN	41,0	1,45%
ND	38,1	1,35%

Εργαζόμενοι με Διγράμματα (1)

- Το πιο συχνό δίγραμμα στα αγγλικά είναι το TH.
- Στο κρυπτογραφημένο μήνυμα, το πιο συχνό δίγραμμα, με 9 εμφανίσεις, είναι το T$\sqcap$, άρα μπορούμε να δοκιμάσουμε την αντικατάσταση του $\sqcap$ από το H.

Αντικατάσταση ⊓ → H

I⊏<O<⌜EA⌞⌞<∨ANTTOHEA⌜A⌴O<TITTHE⊏I⌜∨TTHIN⌝<O
<⌞⌞⌝⌜O⌴A⌴⌞<∨ANTTO⌵NO∨I∨∨HE⌜EI∨A∨⌴O⌜NAN⊐∨
HAT⊐<⌞O<∨<⌞HI⌞⊐HOO⊐∨A∨⌞I⌵EAN⊐HO∨⊐<⌝A⌜ENT
∨∨E⌜EO⌞⌞<⌝IE⊐AN⊐A⌞⌞⌴E⊏O⌜ETHE<HA⊐⊐EAN⊐A⌞⌞T
HAT⊐A∧I⊐⌞O⌝⌝E⌜⊏IE⌞⊐⌵IN⊐O⊏⌞⌜A⌝⌴<TI⊐ONT⊏EE⌞
⌞I⌵E⌝OIN⌝INTOITINTHE⊏I⌜∨T⌝⌞A⌞ETHAT∨T<⊏⊏⌴O⌜E∨
⊐EAN⊐INTHE∨E⌞ON⊐⌝⌞A⌞E⊐<⌝A⌜ENT∨∨O<⌞⊐HA∧EA⌴
O<TT∨OHE⊐O⌜⌜HA⌝E∨A⌝IE⌞EI⊏ITO⌞⊐AN<THIN⌝⌝⌜ETT
<⌝E⌜∨ONA⌞A⌴O<TTHE⊐

Αντικατάσταση

⊓ → H

Εργαζόμενοι με Διγράμματα (2)

- Το δεύτερο πιο συχνό δίγραμμα στο κρυπτογραφημένο κείμενο είναι το $\ulcorner\cdot$ E με 8 εμφανίσεις.
- Στα Αγγλικά το RE είναι επίσης συχνό, οπότε μπορούμε να δοκιμάσουμε την αντικατάσταση του $\ulcorner\cdot$ από το R.

Αντικατάσταση ⌜· → R

I⊏<O<REA⌞⌞<∨ANTTOHEARA⊔O<TITTHE⊏IR∨TTHIN⌝<O<⌞⌞⌝RO⊔A⊔⌞<∨ANTTO⊔NO∨I∨∨HEREI∨A∨⊔ORNAN⊐∨HAT⊐<⌞O<∨<⌞HI⌞⊐HOO⊐∨A∨⌞I⊔EAN⊐HO∨⊐<⌝ARENT∨∨EREO⌞⌞<⌝IE⊐AN⊐A⌞⌞⊔E⊏ORETHE<HA⊐⊐EAN⊐A⌞⌞THAT⊐A∧I⊐⌞O⌝⌝ER⊏IE⌞⊐⊔IN⊐O⊏⌞RA⌝⊔<TI⊐ONT⊏EE⌞⌞I⊔E⌝OIN⌝INTOITINTHE⊏IR∨T⌝⌞A⌞ETHAT∨T<⊏⊏⊔ORE∨⊐EAN⊐INTHE∨E⌞ON⊐⌝⌞A⌞E⊐<⌝ARENT∨∨O<⌞⊐HA∧EA⊔O<TT∨OHE⊐ORRHA⌝E∨A⌝IE⌞EI⊏ITO⌞⊐AN<THIN⌝⌝RETT<⌝ER∨ONA⌞A⊔O<TTHE⊐

Αντικατάσταση

⌜· → R

Μαντεύοντας Λέξεις (1)

- Στην πρώτη γραμμή μπορούμε να δούμε τη σειρά REA𐤋𐤋𐤀.
- Μήπως αυτό σημαίνει REALLY;

Αντικατάσταση ⌞ → L, < → Y

I⊏YO<REALLYVANTTOHEARA⊔O<TITTHE⊏IRVTTHIN⌝YO<LL⌝
RO⊔A⊔LYVANTTO⊔NOVIVVHEREIVAV⊔ORNAN⊐VHAT⊐YLO
<VY⌞HIL⊐HOO⊐VAVLI⊔EAN⊐HOV⊐Y⌝ARENTVVEREO⌞⌞<
⌝IE⊐AN⊐ALL⊔E⊏ORETHEYHA⊐⊐EAN⊐ALLTHAT⊐A∧I⊐⌞O⌝⌝
ER⊏IEL⊐⊔IN⊐O⊏⌞RA⌝⊔<TI⊐ONT⊏EELLI⊔E⌝OIN⌝INTOITINT
HE⊏IRVT⌝LA⌞ETHATVT<⊏⊏⊔OREV⊐EAN⊐INTHEVE⌞ON⊐⌝
LA⌞E⊐Y⌝ARENTVVO<L⊐HA∧EA⊔O<TTVOHE⊐ORRHA⌝EVA⌝
IE⌞EI⊏ITOL⊐ANYTHIN⌝⌝RETTY⌝ERVONALA⊔O<TTHE⊐

Αντικατάσταση

⌞ → L, < → Y

Μαντεύοντας Λέξεις (2)

- Στις πρώτες δύο γραμμές βλέπουμε δύο YO$<$, που μάλλον θα είναι YOU.
- Στην τελευταία γραμμή βλέπουμε το ANYTHIN$\urcorner$, το οποίο μάλλον θα είναι ANYTHING.
- Επίσης στην τελευταία γραμμή το $\urcorner$RETTY είναι μάλλον PRETTY.
- Συνεχίζοντας με αυτόν τον τρόπο, μπορούμε να αποκρυπτογραφήσουμε το μήνυμα στο σύνολό του.

Το Μήνυμα Αποκωδικοποιημένο

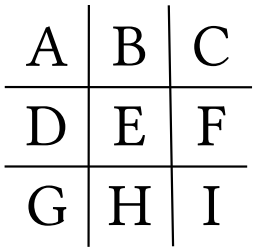
IFYOUREALLYWANTTOHEARABOUTITTHEFIRSTTHINGYOULLPROBA
BLYWANTTOKNOWISWHEREIWASBORNANDWHATMYLOUSYCHILDH
OODWASLIKEANDHOWMYPARENTSWEREOCCUPIEDANDALLBEFORE
THEYHADMEANDALLTHATDAVIDCOPPERFIELDKINDOFCRAPBUTIDO
NTFEELLIKEGOINGINTOITINTHEFIRSTPLACETHATSTUFFBORESMEA
NDINTHESECONDPLACEMYPARENTSWOULDHAVEABOUTTWOHEMO
RRHAGESAPIECEIFITOLDANYTHINGPRETTYPERSONALABOUTTHEM

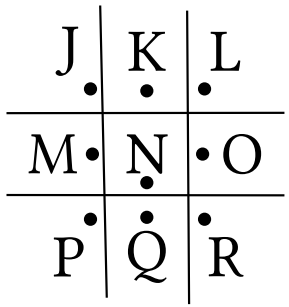
Με Σημεία Στίξης

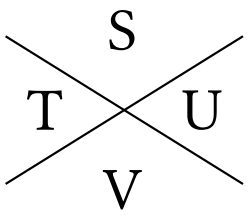
If you really want to hear about it, the first thing you'll probably want to know is where I was born, and what my lousy childhood was like, and how my parents were occupied and all before they had me, and all that David Copperfield kind of crap, but I don't feel like going into it. In the first place, that stuff bores me, and in the second place, my parents would have about two hemorrhages apiece if I told anything pretty personal about them.

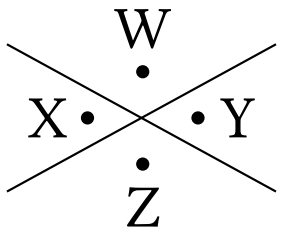
J. D. Salinger, "The Catcher in the Rye".

Ο Κώδικας Pigpen









Επισκόπηση

Γενικά

- Ο κώδικας Vigenère αντιπροσωπεύει τον πιο προχωρημένο κώδικα αντικατάστασης.
- Αντί να βασίζεται σε έναν κανόνα αντικατάστασης, το οποίο είναι εύκολο να αποκρυπτογραφήσουμε με ανάλυση συχνοτήτων, χρησιμοποιεί τόσους κανόνες αντικατάστασης όσα είναι τα γράμματα της αλφαβήτου.

Ιστορία

- Η ιδέα προήλθε από τον Giovan Battista Bellaso στο βιβλίο του, (έκδοση: 1553) La cifra del. Sig. Giovan Battista Bellaso.
- Αποδίδεται όμως, στον Blaise de Vigenère (5 Απριλίου 1523–19 Φεβρουαρίου 1596), ο οποίος ανέπτυξε μια ισχυρότερη μέθοδο από το Bellaso το 1586.

Ιστορία

Blaise de Vigenère (5 Απριλίου 1523–19 Φεβρουαρίου 1596)

https://upload.wikimedia.org/wikipedia/commons/1/1a/Vigenere.jpg

Πίνακας Vigenère

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

Κρυπτογράφηση Vigenère

- Για να κρυπτογραφήσουμε κάτι με τη μέθοδο Vigenère, επιλέγουμε μια κωδική λέξη, ένα κλειδί, και την επαναλαμβάνουμε τόσες φορές όσες χρειαζόμαστε για να φτάσουμε το μήκος του κειμένου που θέλουμε να κρυπτογραφήσουμε.
- Για παράδειγμα, αν το κείμενο που θέλουμε να κρυπτογραφήσουμε είναι:
  ATTACKATDAWN
- Το κλειδί θα είναι:
  LEMON
  άρα για την κρυπτογράφηση θα χρησιμοποιήσουμε:
  LEMONLEMONLE

Κρυπτογράφηση Vigenère (Συνέχεια)

- Για κάθε γράμμα που θέλουμε να κρυπτογραφήσουμε, βρίσκουμε τον αντίστοιχο χαρακτήρα του κλειδιού.
- Βρίσκουμε τη γραμμή που αντιστοιχεί στον χαρακτήρα του κλειδιού.
- Στη συνέχεια βρίσκουμε τη στήλη που αντιστοιχεί στον χαρακτήρα του κειμένου που θέλουμε να κρυπτογραφήσουμε.
- Η τομή της γραμμής και της στήλης μας δίνει το αποτέλεσμα της κρυπτογράφησης για το συγκεκριμένο γράμμα.

Κρυπτογράφηση Vigenère (Συνέχεια)

- Βλέπουμε ότι με τον τρόπο αυτό πράγματι χρησιμοποιούνται τόσα διαφορετικά αλφάβητα κωδικοποίησης όσο είναι και το μήκος του κλειδιού.
- Για το λόγο αυτό η κρυπτογράφηση Vigenère ονομάζεται *πολυαλφαβητική αντικατάσταση* (polyalphabetic substitution).

Παράδειγμα Κρυπτογράφησης Vigenère (1)

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

L E M O N L E M O N L E

A T T A C K A T D A W N

L

Παράδειγμα Κρυπτογράφησης Vigenère (2)

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

L E M O N L E M O N L E

A T T A C K A T D A W N

L X

Παράδειγμα Κρυπτογράφησης Vigenère (3)

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

L E M O N L E M O N L E

A T T A C K A T D A W N

L X F

Παράδειγμα Κρυπτογράφησης Vigenère (4)

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

L E M O N L E M O N L E

A T T A C K A T D A W N

L X F O

Παράδειγμα Κρυπτογράφησης Vigenère (5)

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

L E M O N L E M O N L E

A T T A C K A T D A W N

L X F O P

Παράδειγμα Κρυπτογράφησης Vigenère (6)

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

L E M O N L E M O N L E

A T T A C K A T D A W N

L X F O P V

Αποκρυπτογράφηση Vigenère

- Για κάθε γράμμα που θέλουμε να αποκρυπτογραφήσουμε, βρίσκουμε το αντίστοιχο γράμμα του κλειδιού.
- Στη συνέχεια βρίσκουμε τη γραμμή που αντιστοιχεί στο γράμμα του κλειδιού.
- Βρίσκουμε το κρυπτογραφημένο γράμμα στη γραμμή αυτή.
- Η στήλη που το βρήκαμε είναι το αποκρυπτογραφημένο γράμμα.

Παράδειγμα Αποκρυπτογράφησης Vigenère (1)

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

L E M O N L E M O N L E

L X F O P V E F R N H R

A

Παράδειγμα Αποκρυπτογράφησης Vigenère (2)

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

L E M O N L E M O N L E

L X F O P V E F R N H R

A T

Παράδειγμα Αποκρυπτογράφησης Vigenère (3)

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

L E M O N L E M O N L E
L X F O P V E F R N H R
A T T

Παράδειγμα Αποκρυπτογράφησης Vigenère (4)

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

L E M O N L E M O N L E

L X F O P V E F R N H R

A T T A

Παράδειγμα Αποκρυπτογράφησης Vigenère (5)

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

L E M O N L E M O N L E

L X F O P V E F R N H R

A T T A C

Κρυπτανάλυση του Κώδικα Vigenère (1)

- Επί αιώνες, ο κώδικας Vigenère δεν μπορούσε να παραβιαστεί και ως εκ τούτου είχε ονομαστεί *ο απαραβίαστος κώδικας* (le chiffre indéchiffrable).
- Τελικά αναλύθηκε επιτυχώς από τον Charles Babbage (1854) και τον Friedrich Kasiski (1863).
- Ο Babbage δεν δημοσίευσε τη μέθοδό του, άρα η πρώτη που έγινε γνωστή ήταν του Kasiski. Μετά από χρόνια διαπιστώθηκε ότι ήταν παρόμοιες.

Κρυπτανάλυση του Κώδικα Vigenère (2)

C	A	K	E	C	A	K	E	C	A	K	E	C	A	K	E	C	A	K	E	C	A	K	E	C	A	K	E
C	R	Y	P	T	O	I	S	S	H	O	R	T	F	O	R	C	R	Y	P	T	O	G	R	A	P	H	Y
E	R	I	T	V	O	S	W	U	H	Y	V	V	F	Y	V	E	R	I	T	V	O	Q	V	C	P	R	C

- Στην παραπάνω κρυπτογράφηση με κλειδί «CAKE» βλέπουμε ότι στο κρυπτογραφημένο μήνυμα επαναλαμβάνεται η συμβολοσειρά «ERITVO».
- Οι δύο επαναλήψεις βρίσκονται 16 χαρακτήρες μακριά.
- Αυτό σημαίνει ότι το κλειδί θα έχει μήκος παράγοντα του 16, δηλαδή: 1, 2, 4, 8, 16.
- Μπορούμε να απορρίψουμε το 1 και το 2 γιατί είναι πολύ μικρά.

Κρυπτανάλυση του Κώδικα Vigenère (3)

- Έστω ότι το υποψήφιο μήκος κλειδιού είναι x.
- Τότε αν πάρουμε κάθε x χαρακτήρες του κειμένου:

1	2	3	...	x
$1+x$	$2+x$	$3+x$	...	$x+x$
$1+2x$	$2+2x$	$3+2x$	...	$x+2x$
...	...	...	...	...

οι χαρακτήρες σε κάθε στήλη είναι είναι κωδικοποιημένοι με τον ίδιο κώδικα αντικαστάστασης.

Κρυπτανάλυση του Κώδικα Vigenère (4)

E	R	I	T
V	O	S	W
U	H	Y	V
V	F	Y	V
E	R	I	T
V	O	Q	V
C	P	R	C

- Αν πιστεύουμε ότι το κλειδί έχει μέγεθος 4, τότε γράφουμε το κρυπτογραφημένο μήνυμα σε τέσσερεις στήλες.
- Δοκιμάζουμε κρυπτανάλυση χρησιμοποιώντας συχνότητες εμφάνισης χαρακτήρων *ανά στήλη*.
- Αν έχουμε δίκιο για το μέγεθος του κλειδιού, κάθε στήλη είναι κρυπτογραφημένη με έναν απλό κώδικα αντικατάστασης.

Κρυπτανάλυση του Κώδικα Vigenère (Συνέχεια)

Για κάθε δυνατό μήκος κλειδιού κάνουμε το εξής:

- Βάζουμε το κρυπτογραφημένο κείμενό μας σε έναν πίνακα με τόσες στήλες όσο το μήκος του κλειδιού.
- Τότε οι στήλες του πίνακα αντιστοιχούν σε κείμενο που είναι κρυπτογραφημένο με ένα μόνο αλφάβητο, άρα μπορούμε να το αναλύσουμε με ανάλυση συχνοτήτων.

Εντοπίζουμε το μήκος κλειδιού που βγάζει λογικά αποτελέσματα.

Επισκόπηση

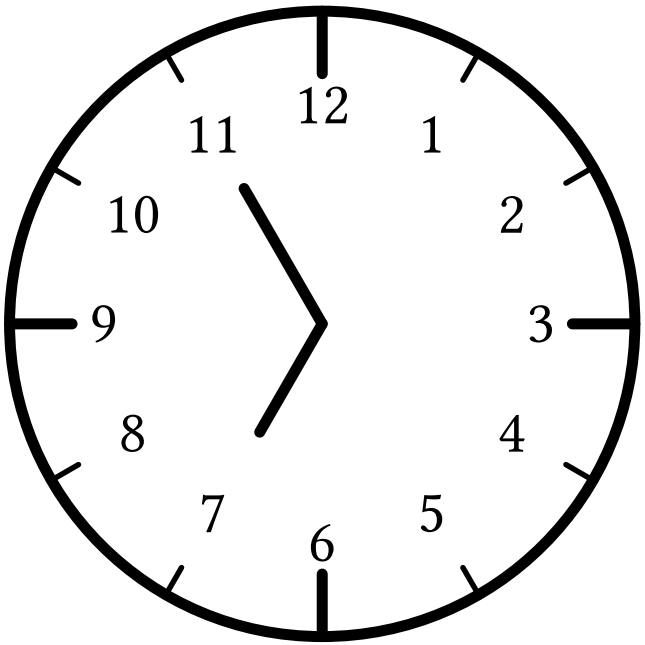
Λειτουργία

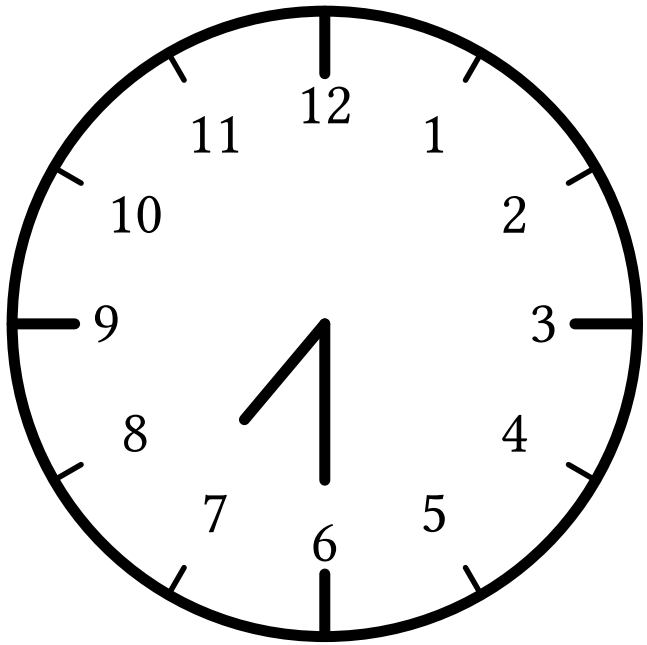
- Στο σημειωματάριο μιας χρήσης χρησιμοποιούμε μια *τυχαία* συμβολοσειρά, ίδιου μήκους με το μήνυμα που θέλουμε να κρυπτογραφήσουμε. Η τυχαία συμβολοσειρά είναι το σημειωματάριο μιας χρήσης.
- Παίρνουμε με τη σειρά ένα χαρακτήρα από το σημειωματάριο μιας χρήσης και ένα χαρακτήρα από το μήνυμά μας.
- Προσθέτουμε τους δύο χαρακτήρες, και παίρνουμε το υπόλοιπο της διαίρεσης του αθροίσματος με το μέγεθος του αλφαβήτου.

Αριθμητική Υπολοίπων (Modular Arithmetic)

- Η αριθμητική υπολοίπων είναι αντίστοιχη με τις πράξεις με λεπτά, όταν προσθέτουμε σε χρονικές στιγμές.
- Το σύμβολο για την πρόσθεση υπολοίπου είναι mod (modulo), και άρα έχουμε $23 \bmod 5 = 3$ αφού το υπόλοιπο του 23 δια του 5 είναι το 3.

Πρόσθεση Λεπτών





Κρυπτογράφηση και Αποκρυπτογράφηση

- Το i γράμμα του κειμένου, $m[i]$, προστίθεται modulo 26 (αφού έχουμε 26 γράμματα στο αγγλικό αλφάβητο) με το i γράμμα του σημειωματαρίου.
- Τα γράμματα τα αντιστοιχούμε σε αριθμούς ξεκινώντας από το μηδέν, δηλαδή A = 0, B = 1, κ.λπ.
- Έτσι έχουμε $c[i] = (m[i] + t[i]) \bmod 26$.
- Η αποκρυπτογράφηση είναι $m[i] = (c[i] - t[i]) \bmod 26$.

Ορισμός $x \bmod y$

Ορισμός

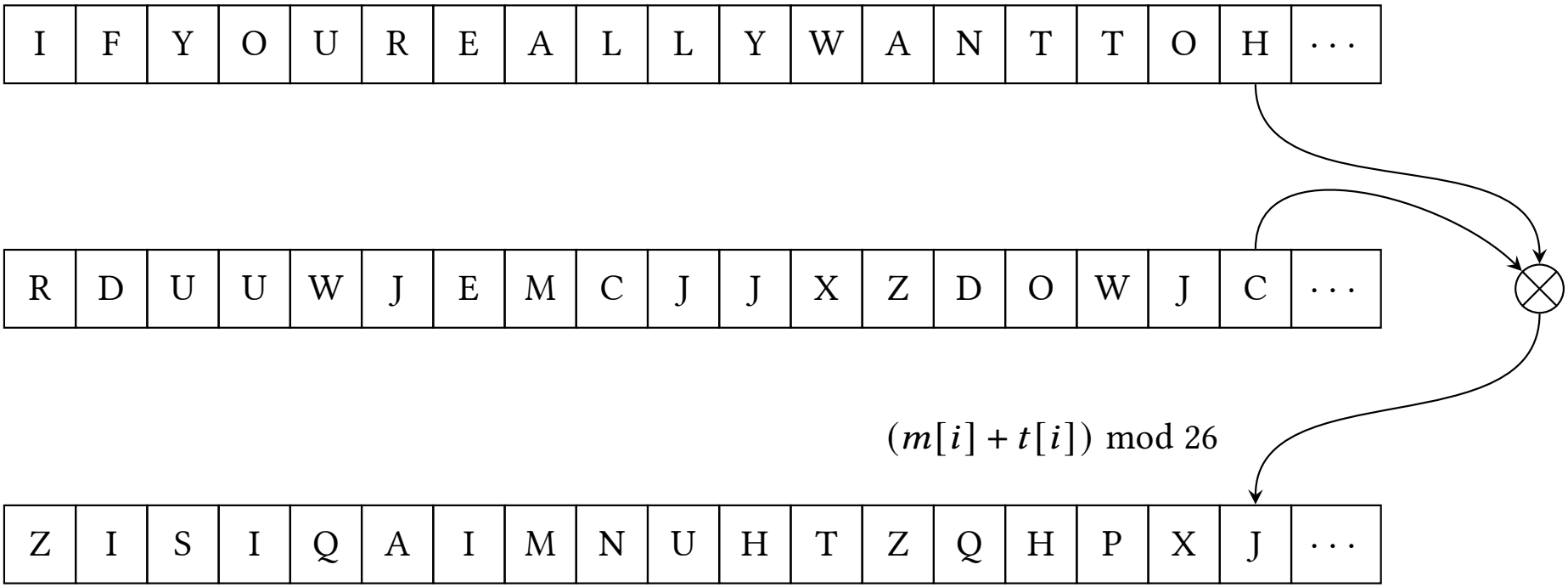
Ο αριθμός $x \bmod y$ είναι ο ακέραιος $r \geq 0$ τέτοιος ώστε $x = qy + r$, όπου q είναι το πηλίκο της διαίρεσης x/y στρογγυλεμμένο προς τα κάτω.

Ο ορισμός αυτός καλύπτει και περιπτώσεις με αρνητικό υπόλοιπο.
Πράγματι, $-6 \bmod 10 = 4$ γιατί $\lfloor -6/10 \rfloor = -1$ και
$r = -6 - 10(-1) = -6 + 10 = 4$

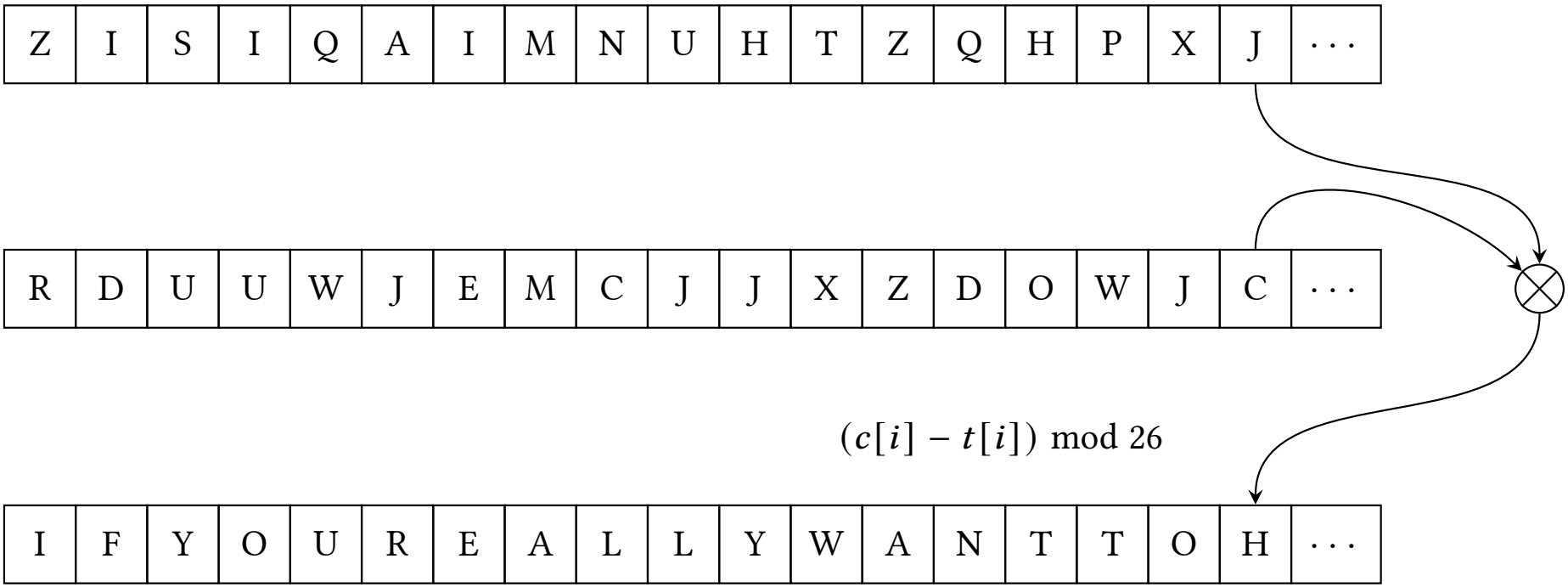
Ασφάλεια Σημειωματαρίου Μιας Χρήσης

- Το σημειωματάριο μιας χρήσης είναι απολύτως ασφαλές και απαραβίαστο.
- Μόνο με τη χρήση του σημειωματαρίου μπορεί να αποκρυπτογραφηθεί το μήνυμα σωστά.
- Χωρίς το σημειωματάριο, κάθε αποκρυπτογράφηση είναι εξίσου πιθανή!

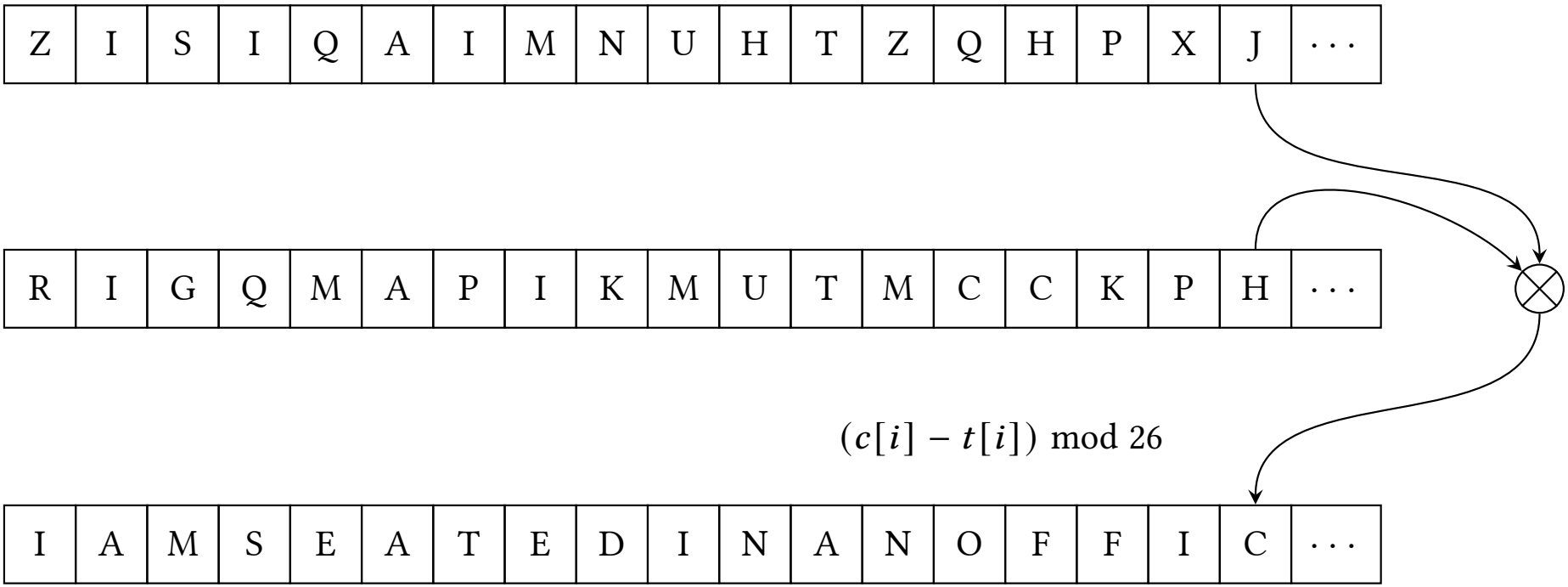
Παράδειγμα


I F Y O U R E A L L Y W A N T T O H ···
R D U U W J E M C J J X Z D O W J C ···
$(m[i] + t[i]) \bmod 26$
Z I S I Q A I M N U H T Z Q H P X J ···

Σωστή Αποκρυπτογράφηση



Λάθος Αποκρυπτογράφηση



Αποκλειστικό Ή (Exclusive Or, XOR)

		x	
		0	1
y	0	0	1
	1	1	0

- Το αποκλειστικό ή (exclusive or, XOR) είναι μια δυαδική πράξη η οποία δίνει 1 αν οι δύο παράμετροι είναι διαφορετικές, 0 αν είναι ίδιες.
- Συμβολίζεται με $\oplus$.
- Έχουμε $1 \oplus 1 = 0 \oplus 0 = 0$, $1 \oplus 0 = 0 \oplus 1 = 1$.
- Το XOR έχει την ιδιότητα: αν $c = a \oplus b$, τότε $c \oplus b = a$.

Σημειωματάριο Μιας Χρήσης με XOR

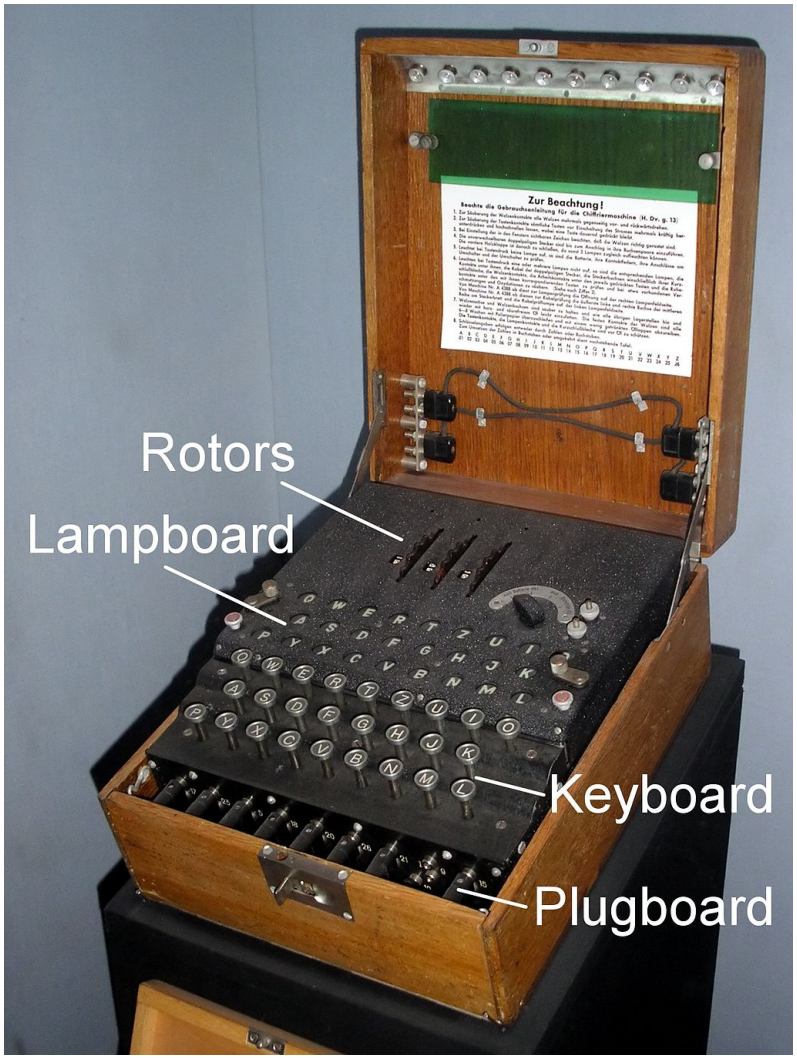
- Κάθε χαρακτήρας αναπαρίσταται από έναν δυαδικό αριθμό, π.χ. το A είναι το 1100001 στον κώδικα ASCII.
- Το σημειωματάριο είναι μια τυχαία δυαδική ακολουθία, όπως 1101011....
- Το κρυπτογραφημένο μήνυμα προκύπτει παίρνοντας το XOR του αρχικού μηνύματος με το σημειωματάριο, bit προς bit.
- Στην περίπτωσή μας, $1100001 \oplus 1101011 = 0001010$.
- Για την αποκρυπτογράφηση χρησιμοποιούμε πάλι XOR του κρυπτογραφημένου μηνύματος με το σημειωματάριο: $0001010 \oplus 1101011 = 1100001$.

Προβλήματα Σημειωματαρίου Μιας Χρήσης

- Τα σημειωματάρια μιας χρήσης πολύ δύσκολα χρησιμοποιούνται στην πράξη.
- Πρέπει το σημειωματάριο να είναι *απολύτως τυχαίο*.
- Πρέπει το σημειωματάριο να είναι *μοναδικό*.
- Πρέπει το σημειωματάριο να έχει μήκος τουλάχιστον όσο το μήνυμα.

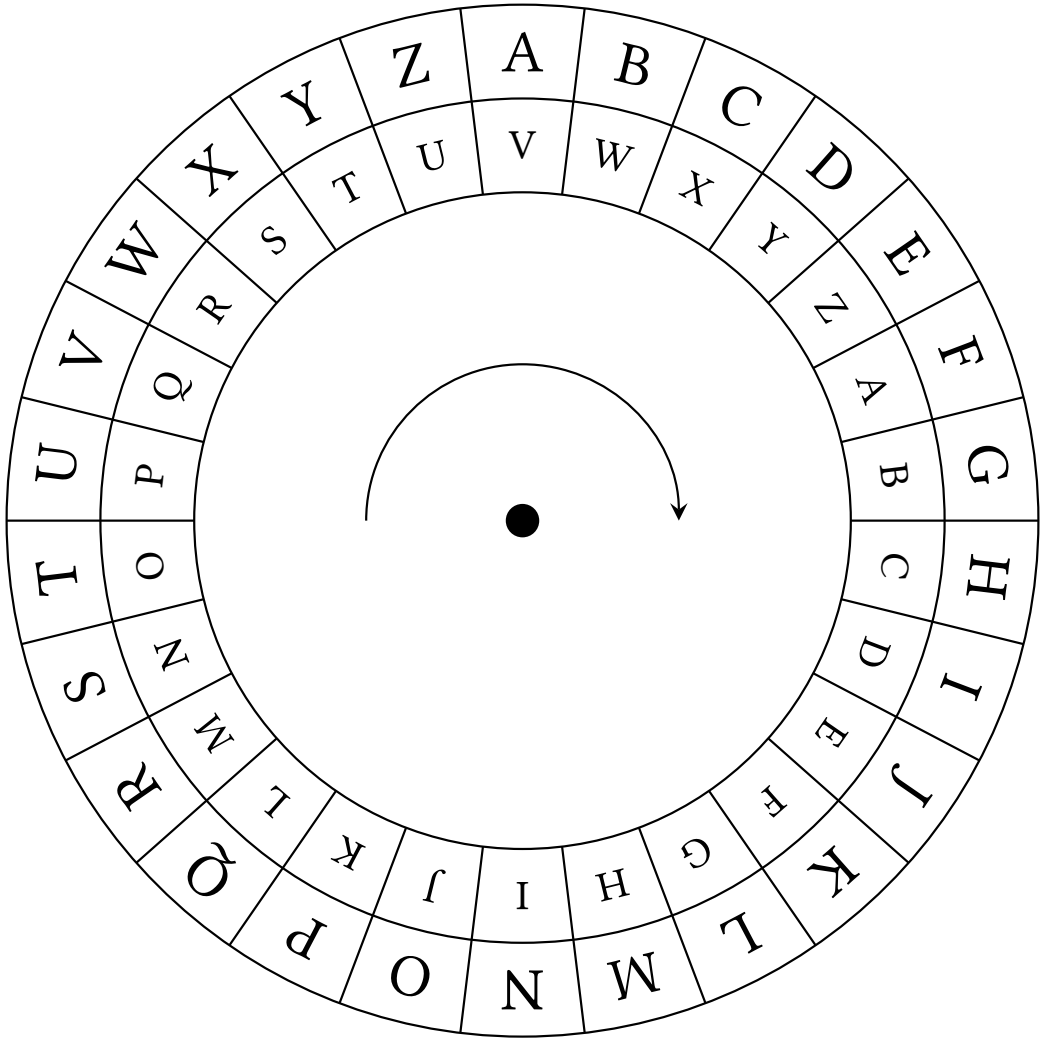
Επισκόπηση

Η Κρυπτογραφική Μηχανή Enigma

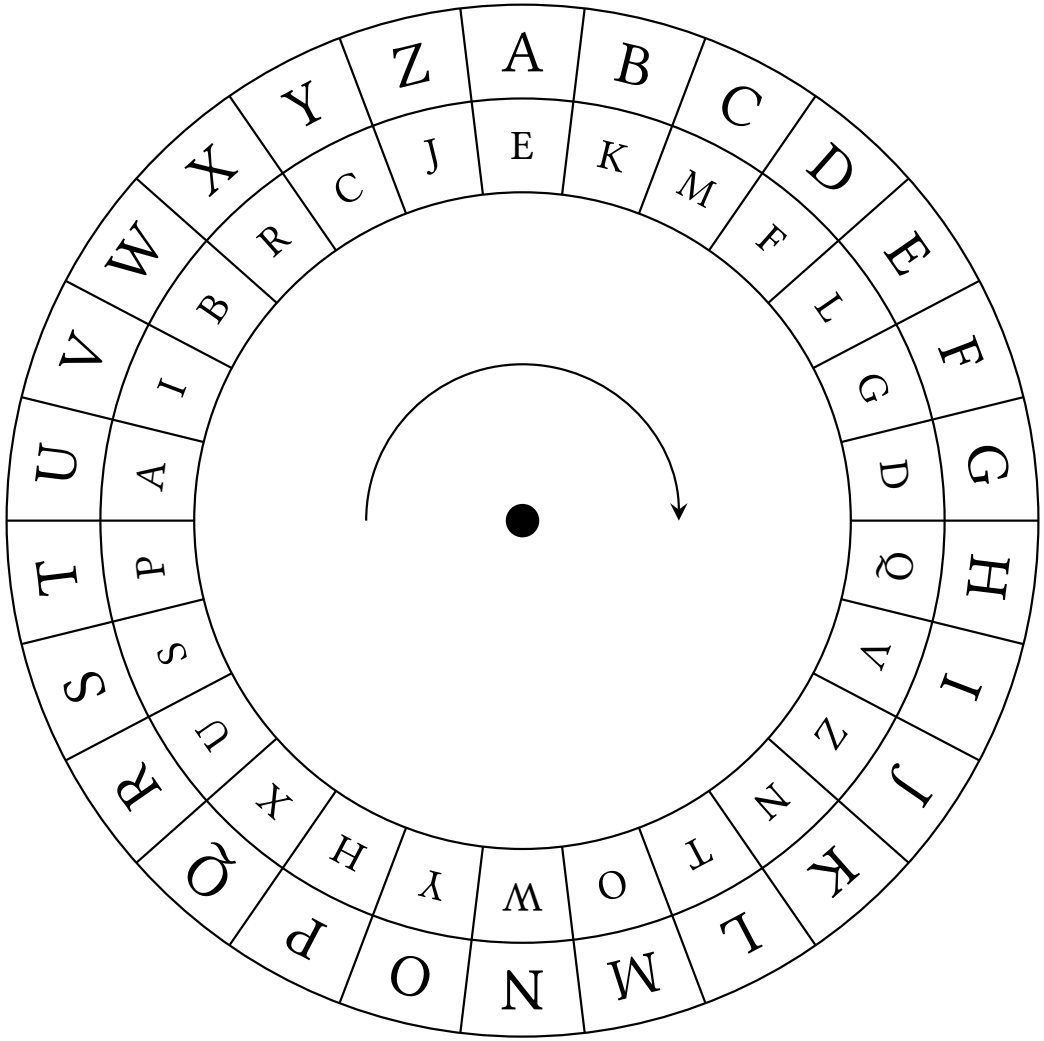


http://upload.wikimedia.org/wikipedia/commons/3/3e/EnigmaMachineLabeled.jpg

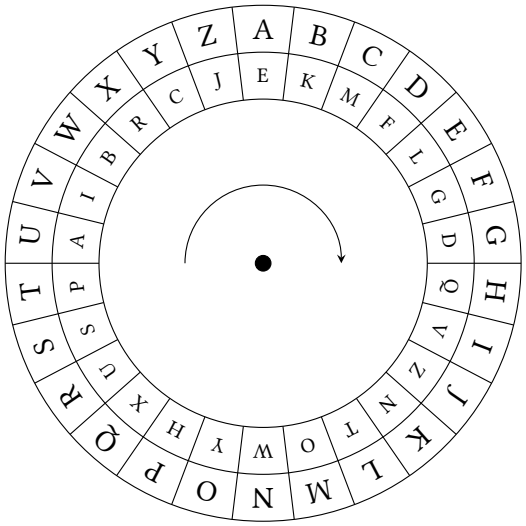
Κρυπτογραφικός Δίσκος (Cipher Disk)



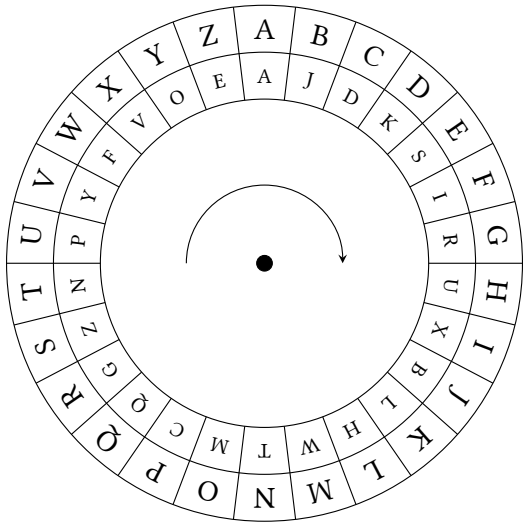
Κρυπτογραφικός Δίσκος Με Τυχαία Διάταξη



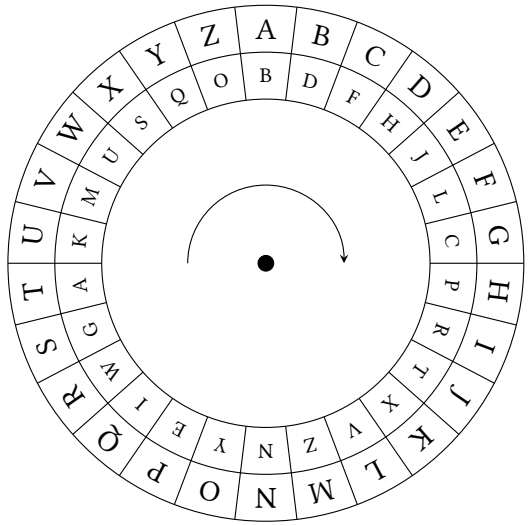
Σειρά Δίσκων



Γυρνάει μία θέση ανά χαρακτήρα.

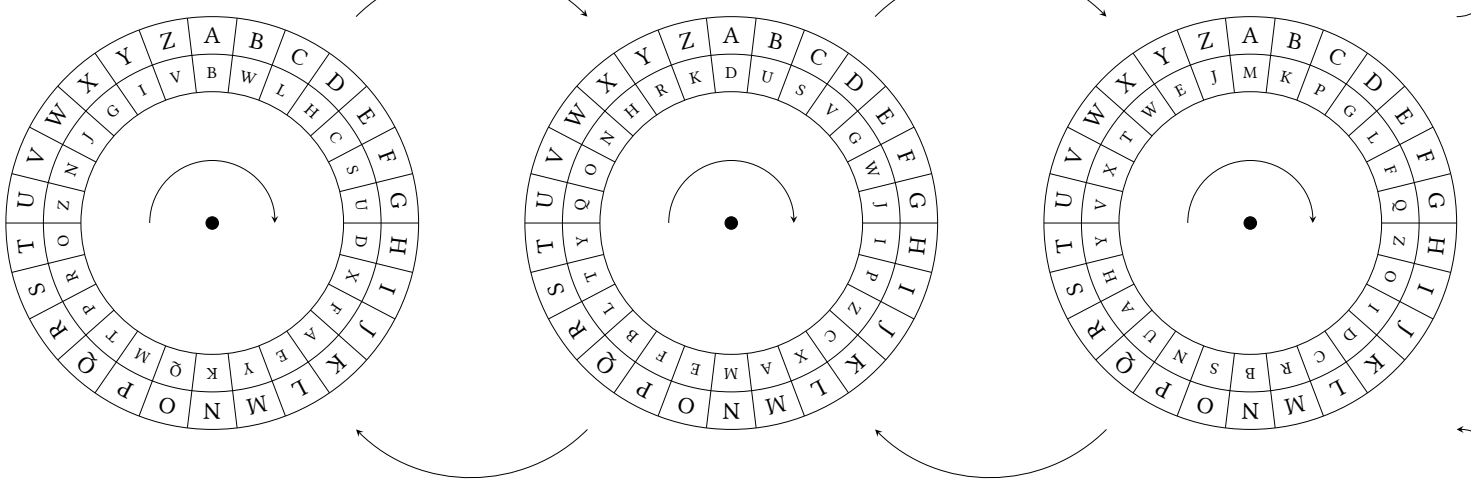


Γυρνάει μία θέση για μία περιστροφή του προηγούμενου.



Γυρνάει μία θέση για μία περιστροφή του προηγούμενου.

Δομή Enigma



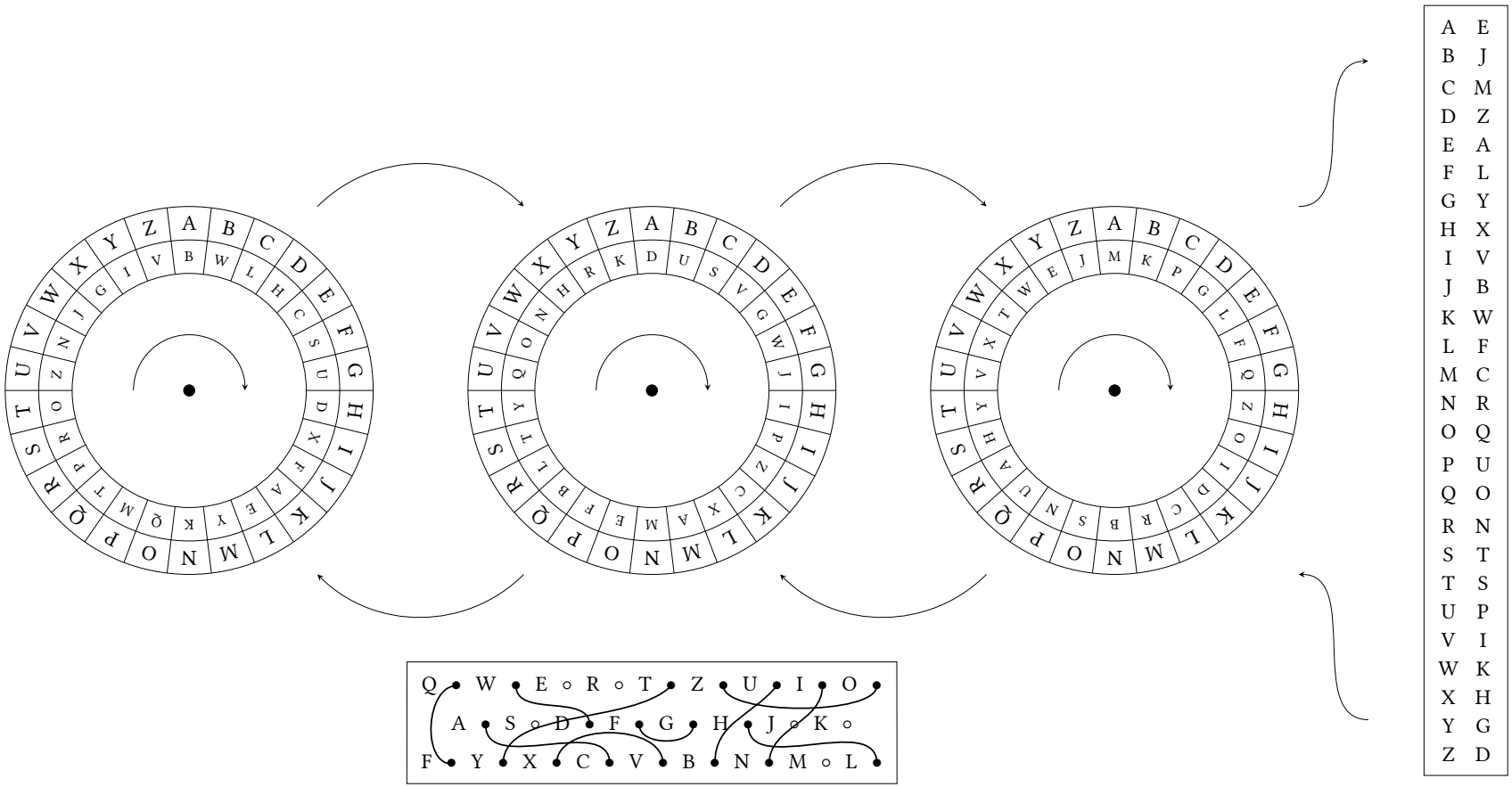
A	E
B	J
C	M
D	Z
E	A
F	L
G	Y
H	X
I	V
J	B
K	W
L	F
M	C
N	R
O	Q
P	U
Q	O
R	N
S	T
T	S
U	P
V	I
W	K
X	H
Y	G
Z	D

Q ∘ W ∘ E ∘ R ∘ T ∘ Z ∘ U ∘ I ∘ O ∘

A ∘ S ∘ D ∘ F ∘ G ∘ H ∘ J ∘ K ∘

F ∘ Y ∘ X ∘ C ∘ V ∘ B ∘ N ∘ M ∘ L ∘

Παράδειγμα Enigma



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

$$W \rightarrow D$$
$$D \rightarrow H \rightarrow I \rightarrow O$$
$$O \rightarrow Q$$
$$Q \rightarrow G \rightarrow E \rightarrow L$$
$$L \rightarrow H$$

Ανάλυση Πολυπλοκότητας Enigma

- Θέσεις δίσκων:

$$26 \times 26 \times 26 = 17.576$$

- Διατάξεις δίσκων: Οι 3 δίσκοι μπορούν να διαταχθούν με 6 διαφορετικούς τρόπους: 123, 132, 213, 231, 312, 312.

Ανάλυση Πολυπλοκότητας Enigma (Συνέχεια)

- Επιλογή δίσκων: το σύνολο των δίσκων στις συσκευές του στρατού ξηράς και της αεροπορίας ήταν 5, από τους οποίους επιλέγονται οι 3. Ο αριθμός των επιλογών ήταν:

$$\binom{5}{3} = \frac{5!}{2!3!} = 10$$

- Άρα συνολικά από τους δίσκους και μόνο έχουμε για στρατό ξηράς και αεροπορία:

$$17.576 \times 6 \times 10 = 105.456 \times 10 = 1.054.560$$

Ανάλυση Πολυπλοκότητας Enigma (Συνέχεια)

- Επιλογή δίσκων: στο ναυτικό το σύνολο των δίσκων ήταν 8, άρα ο αριθμός των επιλογών ήταν:

$$\binom{8}{3} = \frac{8!}{3!5!} = 56$$

- Επιπλέον ο ανακλαστήρας δεν ήταν σταθερός, αλλά μπορούσε να πάρει μία από 26 θέσεις.
- Άρα συνολικά:

$$17.576 \times 6 \times 56 \times 26 = 153.543.936$$

Ανάλυση Πολυπλοκότητας Enigma (Συνέχεια)

- Υπάρχουν $\binom{26}{2}$ τρόποι να συνδέσουμε ένα ζευγάρι γραμμάτων.
- Υπάρχουν $\binom{24}{2}$ τρόποι να συνδέσουμε ένα επιπλέον ζευγάρι γραμμάτων.
- Για 10 ζευγάρια γραμμάτων έχουμε:

$$\binom{26}{2}\binom{24}{2}\binom{22}{2}\binom{20}{2}\binom{18}{2}\binom{16}{2}\binom{14}{2}\binom{12}{2}\binom{10}{2}\binom{8}{2}$$

Ανάλυση Πολυπλοκότητας Enigma (Συνέχεια)

- Αυτό, μετά από απλοποιήσεις γίνεται:

$$\frac{26!}{6!2^{10}}$$

- Επειδή δεν έχει σημασία η σειρά των ζευγαριών, πρέπει να διαιρέσουμε με το σύνολο των διατάξεων:

$$\frac{26!}{10!6!2^{10}} = 150.738.274.937.250$$

- Γενικότερα, ο αριθμός των τρόπων με τους οποίους μπορούμε να επιλέξουμε m ζευγάρια από n αντικείμενα είναι:

$$\frac{n!}{m!(n-2m)!2^m}$$

Ανάλυση Πολυπλοκότητας Enigma (Συνέχεια)

Προκύπτει λοιπόν ότι ο αριθμός των δυνατών κλειδών Enigma ήταν:

- Για το στρατό ξηράς και αεροπορία:

$$1.054.560 \times 150.738.274.937.250 = 158.962.555.217.826.360.000$$

ή

$$1{,}5896255521782636 \times 10^{20}$$

ή 158 πεντάκις εκατομμύρια.

- Για το ναυτικό:

$$153.543.936 \times 150.738.274.937.250 = 23.144.948.039.715.518.016.000$$

ή

$$2{,}3144948039715518016^{22}$$

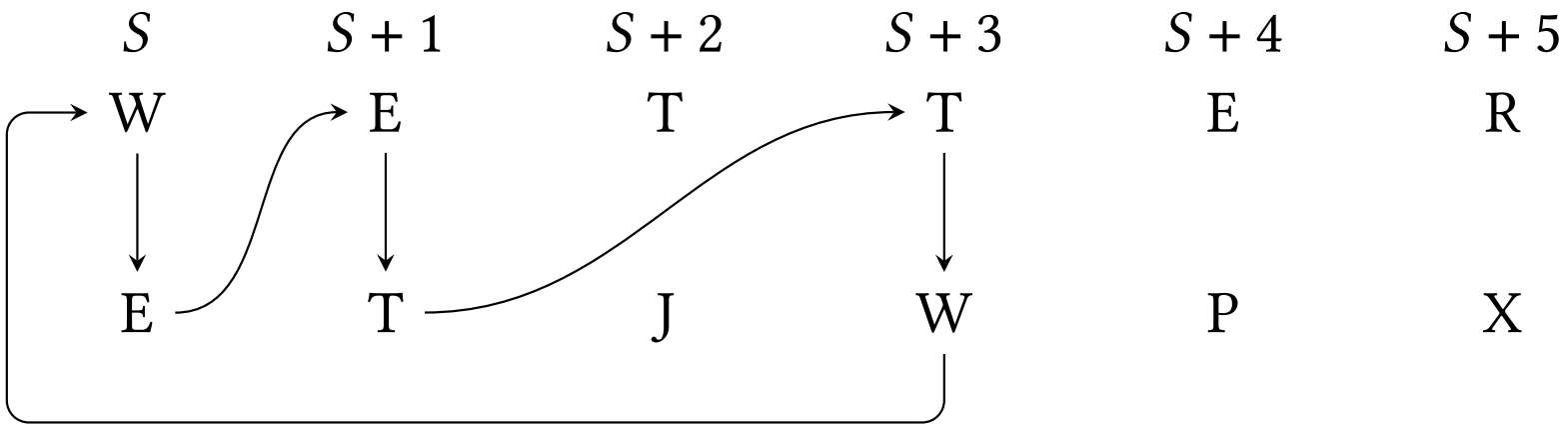
ή 23 εξάκις εκατομμύρια.

Alan Turing

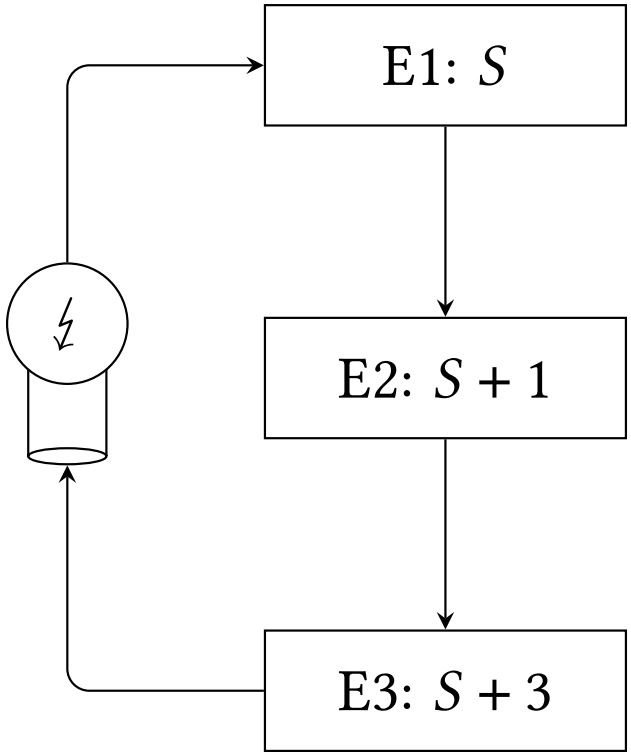
http://upload.wikimedia.org/wikipedia/en/c/c8/Alan_Turing_photo.jpg

Αποκρυπτογράφηση Enigma

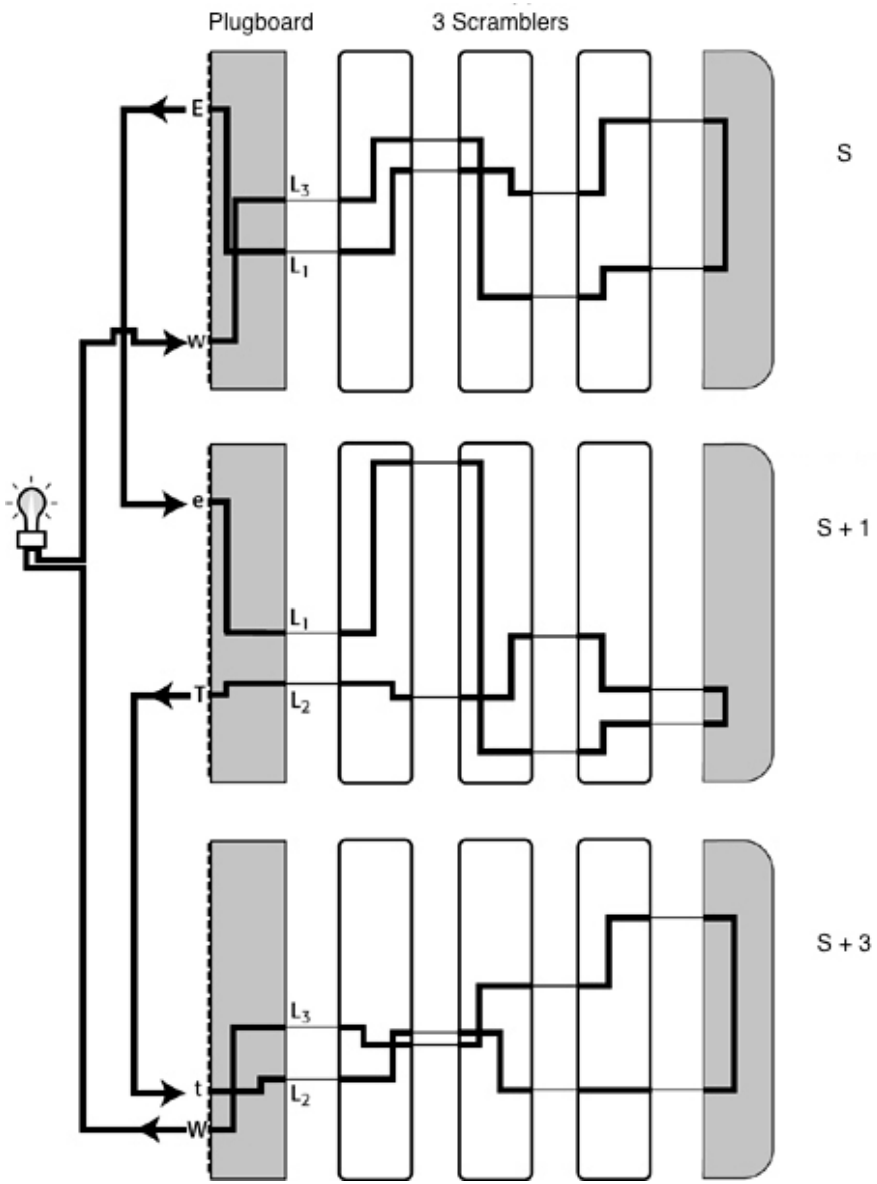
- Προς το παρόν ας αγνοήσουμε τον πίνακα συνδέσεων.
- Έστω ότι έχουμε βρει ένα τμήμα κρυπτογραφημένου μηνύματος μαζί με την αποκρυπτογράφησή του.
- Έστω επίσης ότι παρατηρούμε ένα βρόχο στην κρυπτογράφηση, για παράδειγμα ότι: $\mathrm{W} \to \mathrm{E} \to \mathrm{T} \to \mathrm{W}$.



Αποκρυπτογράφηση Enigma (Συνέχεια)



Αποκρυπτογράφηση Enigma (Συνέχεια)

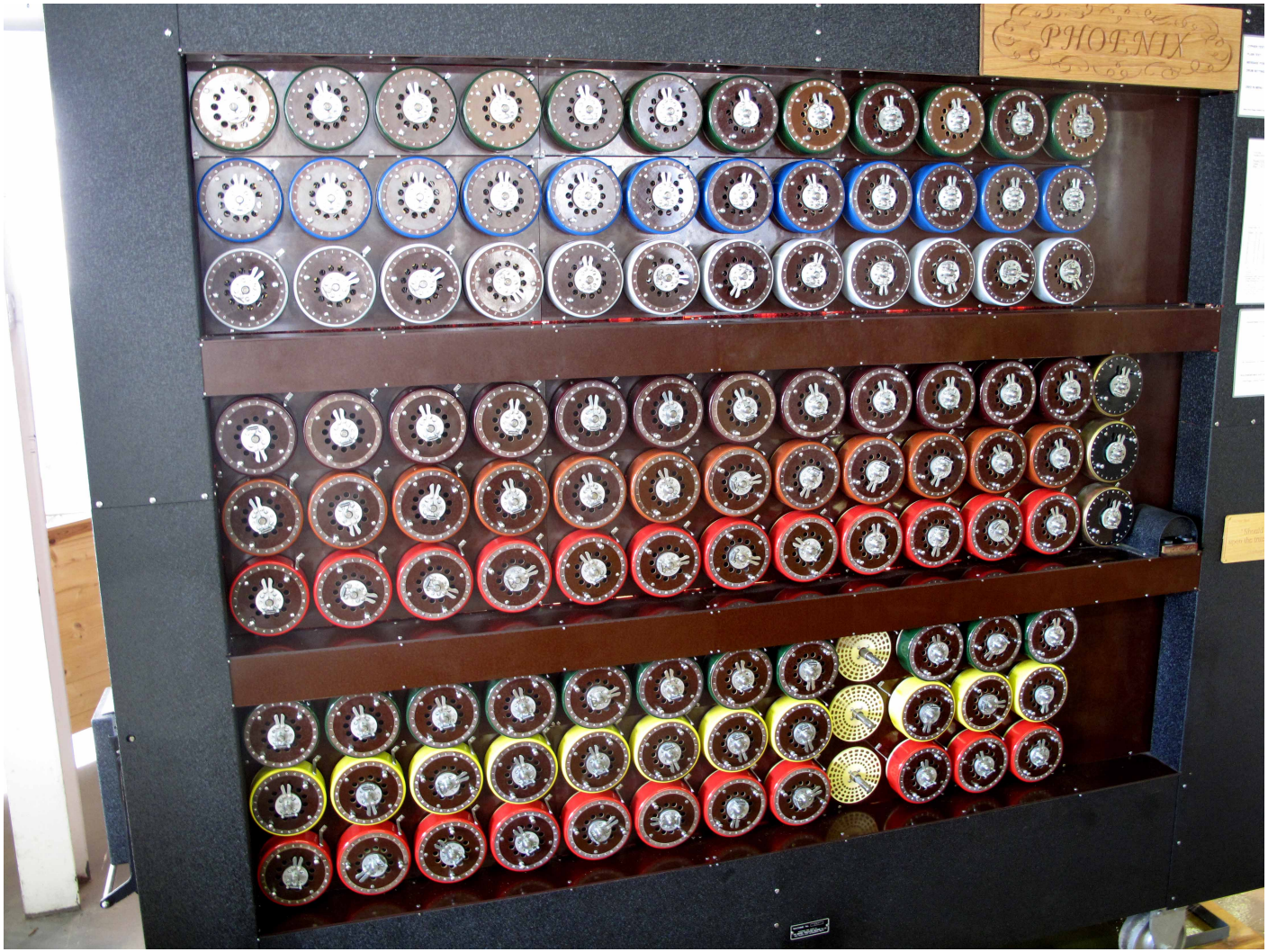


Simon Singh: The Codebook.

Βασικές Ιδέες Αποκρυπτογράφησης

- Η σύνδεση των Enigma στη σειρά σημαίνει ότι οι πίνακες συνδέσεων αλληλοεξουδετερώνονται.
- Άρα αρκούν να δοκιμαστούν 17.756 συνδυασμοί.
- Αν αποτύχουν τότε απλώς δοκιμάζονται άλλοι δίσκοι.
- Εναλλακτικά, μπορούν να δοκιμάζονται περισσότερες μηχανές Enigma παράλληλα.

Bombe



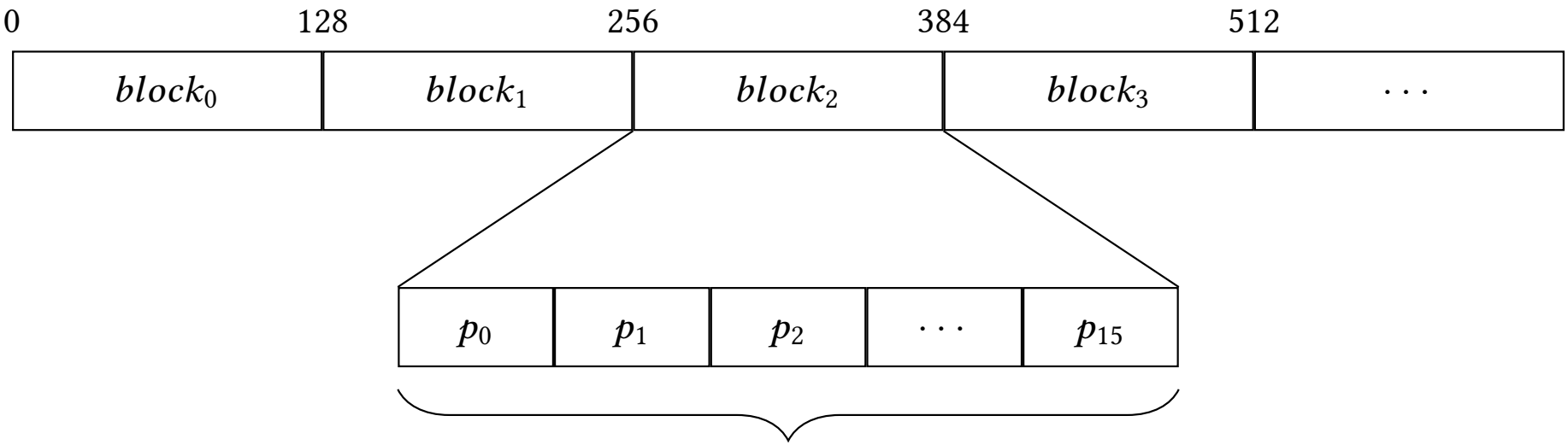
http://upload.wikimedia.org/wikipedia/commons/b/b1/RebuiltBombeFrontView.jpg

Επισκόπηση

Ανάπτυξη του AES

- Το AES είναι πρότυπο που έχει επιλεγεί από το αμερικάνικο National Institute of Standards and Technology (NIST) το 2001.
- Η επιλογή έγινε μέσω ανοιχτής διαδικασίας για την αντικατάσταση ενός παλαιότερου πρότυπου, του Data Encryption Standard (DES).
- Η διαδικασία κράτησε από το 1997 έως το 2000.
- Το NIST προσκάλεσε την κρυπτογραφική κοινότητα να προτείνει αντικαταστάτες.
- Στις 2 Οκτωβρίου 2000 το NIST ανακοίνωσε ότι νικητής ήταν η πρόταση δύο Βέλγων κρυπτογράφων, των Joan Daemen και Vincent Rijmen, με την ονομασία Rijndael.

AES: Κατασκευή Πίνακα Κατάστασης



p_0	p_4	p_8	p_{12}
p_1	p_5	p_9	p_{13}
p_2	p_6	p_{10}	p_{14}
p_3	p_7	p_{11}	p_{15}

AES: AddRoundKey

p_0	p_4	p_8	p_{12}
p_1	p_5	p_9	p_{13}
p_2	p_6	p_{10}	p_{14}
p_3	p_7	p_{11}	p_{15}

k_0	k_4	k_8	k_{12}
k_1	k_5	k_9	k_{13}
k_2	k_6	k_{10}	k_{14}
k_3	k_7	k_{11}	k_{15}

$\oplus$

x_0	x_4	x_8	x_{12}
x_1	x_5	x_9	x_{13}
x_2	x_6	x_{10}	x_{14}
x_3	x_7	x_{11}	x_{15}

AES: Το Κουτί Αντικατάστασης (S-Box)

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

AES: SubBytes

x_0	x_4	x_8	x_{12}
x_1	x_5	x_9	x_{13}
x_2	x_6	x_{10}	x_{14}
x_3	x_7	x_{11}	x_{15}

$s_{0,0}$	$s_{0,1}$	$\cdots$	$s_{0,F}$
$s_{1,0}$	$s_{1,1}$	$\cdots$	$s_{1,F}$
$\cdots$	$\cdots$	$\cdots$	$\cdots$
$s_{F,0}$	$s_{F,1}$	$\cdots$	$s_{F,F}$

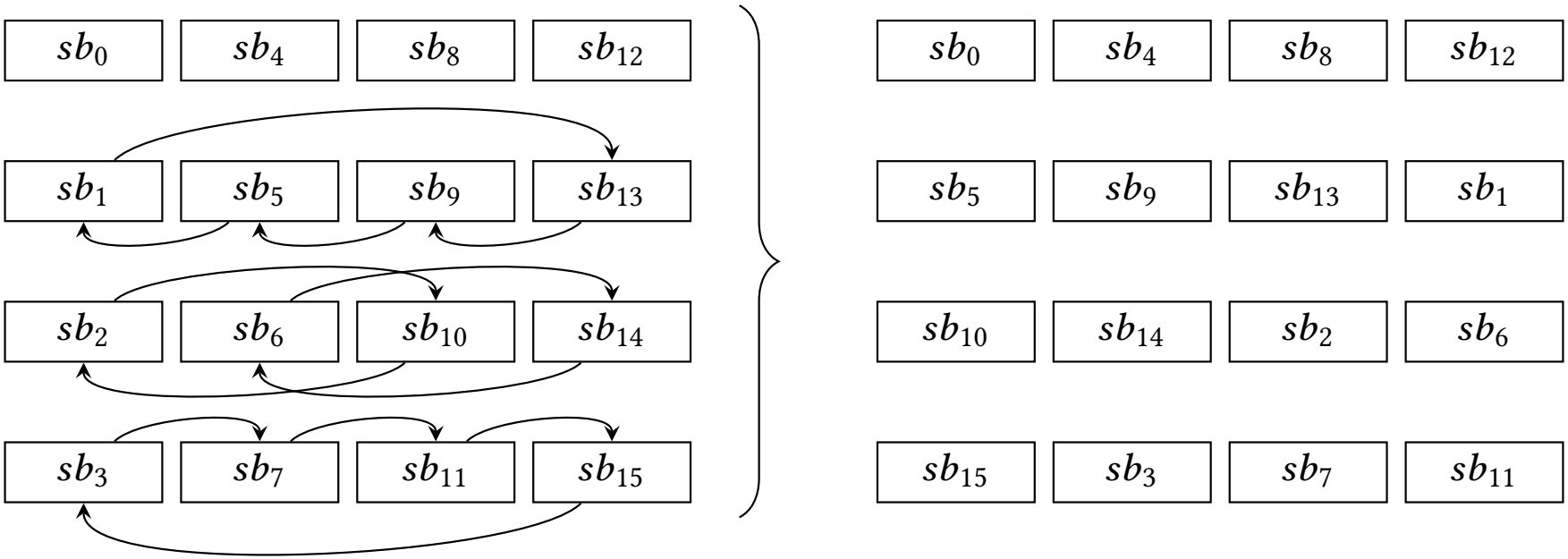
$$x_i = h_1 h_2 \rightarrow sb_i = s_{h_1,h_2}$$

sb_0	sb_4	sb_8	sb_{12}
sb_1	sb_5	sb_9	sb_{13}
sb_2	sb_6	sb_{10}	sb_{14}
sb_3	sb_7	sb_{11}	sb_{15}

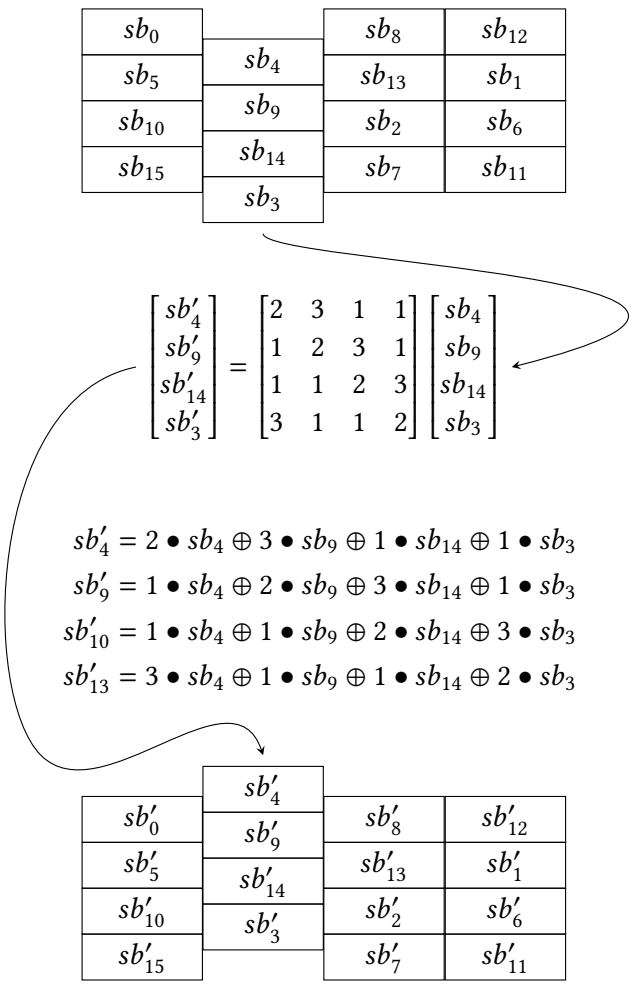
Παράδειγμα: SubBytes

- Έστω $x_4 = 168$.
- 168 στο δεκαδικό είναι A8 στο δεκαεξαδικό.
- Πάμε στη γραμμή A και στήλη 8 του S-box και βρίσκουμε τον αριθμό C2 σε δεκαεξαδικό, ή 194 στο δεκαδικό.
- Άρα $sb_4 = 194$.

AES: ShiftRows



AES: MixColumns



AES: `MixColumns`

- Ο πίνακας είναι ο ίδιος για όλες τις στήλες.
- Ο πολλαπλασιασμός και η πρόσθεση δεν είναι οι συνηθισμένες πράξεις που ξέρουμε.
- Είναι η πρόσθεση και ο πολλαπλασιασμός είναι οι αντίστοιχες «πράξεις υπολοίπων ως προς ένα ανάγωγο πολυώνυμο βαθμού 8 στο πεπερασμένο πεδίο $GF(2^8)$» (addition and multiplication of polynomials modulo an irreducible polynomial of degree 8 in the finite field $GF(2^8)$).

AES: MixColumns

- Η πρόσθεση $\oplus$ είναι απλώς XOR των bits που αναπαριστούν τους παράγοντες.
- Για τον πολλαπλασιασμό πρέπει να δούμε τι σημαίνει πολλαπλασιασμός με το 1, 2, και 3 (αφού μόνο αυτοί οι πολλαπλασιασμοί γίνονται, όπως βλέπουμε στην εικόνα).
- Έχουμε:

$$1 \bullet a = a$$

$$3 \bullet a = 2 \bullet a \oplus a$$

- Άρα χρειάζεται απλώς να δούμε πώς γίνεται ο πολλαπλασιασμός με το 2, $2 \bullet a$.

AES: MixColumns

- Αν η αναπαράσταση του a στο δυαδικό σύστημα είναι: $a = (a_7, a_6, \ldots, a_0)$
- Τότε έχουμε:

$$2 \bullet a = \begin{cases} (a_6, \ldots, a_0, 0) & \text{αν } a_7 = 0 \\ (a_6, \ldots, a_0, 0) \oplus (0, 0, 0, 1, 1, 0, 1, 1) & \text{αν } a_7 = 1 \end{cases}$$

Ο Αλγόριθμος AES

Algorithm: AES cipher algorithm.

`AESCipher`$(b, k, n) \rightarrow s$

Input: b, a block of 16 bytes
k, the encryption key
n, the number of rounds

Data: s, the state
rk, an array of size $n + 1$ that will contain the round keys

Output: s, the ciphertext corresponding to b

```
1  s ← CreateState(b)
2  rk ← ExpandKey(k)
3  s ← AddRoundKey(s, rk[0])
4  for i ← 1 to n do
5      s ← SubBytes(s)
6      s ← ShiftRows(s)
7      s ← MixColumns(s)
8      s ← AddRoundKey(s, rk[i])
9  s ← SubBytes(s)
10 s ← ShiftRows(s)
11 s ← AddRoundKey(s, rk[n])
12 return s
```

Επισκόπηση

Το Πρόβλημα

- Ο AES, όπως και άλλοι σύγχρονοι αλγόριθμοι κρυπτογραφίας, είναι ασφαλής αρκεί να μη διαρρεύσει το κλειδί.
- Συγκεκριμένα, όλη η ασφάλεια επαφείεται στη μυστικότητα του κλειδιού (αρχή του Kerckhoffs, 1883).
- Πώς μπορούμε να μεταδώσουμε με ασφαλή τρόπο το κλειδί στον παραλήπτη;

Παράδειγμα (1)

1. Η Alice και ο Bob συμφωνούν σε δύο αριθμούς, έναν πρώτο αριθμό p, και έναν άλλο, όχι αναγκαστικά πρώτο, g ώστε $2 \leq g \leq p-2$. Έστω ότι $p = 23$ και $g = 14$. Οι δύο αριθμοί δεν είναι ανάγκη να κρατηθούν μυστικοί.
2. Η Alice επιλέγει ένα μυστικό αριθμό a, $1 \leq a \leq p-1$. Έστω ότι επιλέγει $a = 3$. Υπολογίζει τον αριθμό

$$A = g^a \bmod p$$

   ή $14^3 \bmod 23 = 2744 \bmod 23 = 7$.
3. Η Alice στέλνει τον αριθμό A, δηλαδή το 7, στον Bob.

Παράδειγμα (2)

4. Ο Bob επιλέγει ένα μυστικό αριθμό b, $1 \leq b \leq p-1$. Έστω ότι επιλέγει $b = 4$. Κάνει τους ίδιους υπολογισμούς με την Alice, δηλαδή

$$B = g^b \bmod p$$

ή $14^4 \bmod 23 = 38\,416 \bmod 23 = 6$.

5. Ο Bob στέλνει τον αριθμό B, δηλαδή το 6, στην Alice.

Παράδειγμα (3)

6. Η Alice υπολογίζει τον αριθμό

$$B^a \bmod p$$

δηλαδή, $6^3 \bmod 23 = 216 \bmod 23 = 9$.

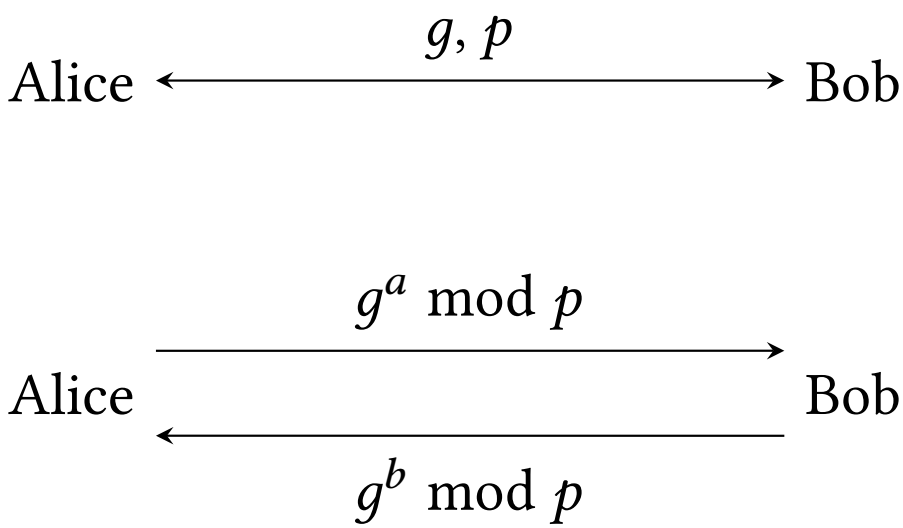
7. Ο Bob υπολογίζει τον αριθμό

$$A^b \bmod p$$

ή $7^4 \bmod 23 = 2401 \bmod 23 = 9$.

8. Το 9 είναι το μυστικό κλειδί της Alice και του Bob.

Επικοινωνία σε Diffie-Hellman



Ανταλλαγή Κλειδιών με Μέθοδο Diffie-Hellman

Alice	Bob
Alice and Bob agree on p and g	
Choose a Calculate $A = g^a \bmod p$ Send A to Bob	Choose b Calculate $B = g^b \bmod p$ Send B to Alice
Calculate $s = B^a \bmod p$ $= (g^b)^a \bmod p$ $= g^{ba} \bmod p$	Calculate $s = A^b \bmod p$ $= (g^a)^b \bmod p$ $= g^{ab} \bmod p$

Ασφάλεια Diffie-Hellman

- Δεν υπάρχει γνωστός αποτελεσματικός τρόπος να βρεθεί το μυστικό μέσω των p, g, A, και B.
- Αυτό ανάγεται στο πρόβλημα του *διακριτού λογάριθμου* (discrete logarithm problem), για το οποίο δεν υπάρχει αποτελεσματική λύση.
- Αν έχουμε έναν πρώτο αριθμό p, έναν αριθμό g, και $y = g^x \bmod p$, το πρόβλημα του διακριτού λογαρίθμου είναι η εύρεση του ακεραίου x, $1 \leq x \leq p - 1$.
- Ο ακέραιος x ονομάζεται *διακριτός λογάριθμος του y με βάση g* και γράφουμε $x = \log_g y \bmod p$.

Μονόδρομες Συναρτήσεις (One-way Functions)

- Η $y = g^x \bmod p$ είναι μια *μονόδρομη συνάρτηση* (one-way function).
- Είναι εύκολο να υπολογίσουμε το y αν έχουμε τα g, x, και p.
- Δεν γνωρίζουμε όμως αποτελεσματική μέθοδο να υπολογίσουμε το x αν ξέρουμε τα y, g, και p.
- Μπορούμε μόνο να δοκιμάσουμε διάφορες τιμές για το x μέχρι να βρούμε τη σωστή.

Συμπεριφορά g^x και $g^x \bmod p$ (1)

Για $g = 2$ και $p = 13$ έχουμε:

x	1	2	3	4	5	6	7	8	9	10	11	12
g^x	2	4	8	16	32	64	128	256	512	1024	2048	4096
$g^x \bmod p$	2	4	8	3	6	12	11	9	5	10	7	1

- Ενώ η συμπεριφορά του 2^x είναι προβλέψιμη, η συμπεριφορά του $2^x \bmod 13$ δεν φαίνεται να είναι.
- Το $2^x \bmod 13$ θα πάρει όλες τις τιμές από το 1 μέχρι και το 12 πριν αρχίσει να επαναλαμβάνεται.

Συμπεριφορά g^x και $g^x \bmod p$ (2)

- Πράγματι:

$$\begin{aligned} 2^{13} \bmod 13 &= (2^{12} \times 2) \bmod 13 \\ &= ((2^{12} \bmod 13) \times (2 \bmod 13)) \bmod 13 \\ &= (1 \times 2) \bmod 13 = 2 \end{aligned}$$

- Και γενικά, μπορούμε να δούμε ότι η συνάρτηση $2^x \bmod 13$ είναι περιοδική με περίοδο 12:

$$\begin{aligned} 2^{12+k} \bmod 13 &= ((2^{12} \bmod 13) \times (2^k \bmod 13)) \bmod 13 \\ &= (1 \times 2^k) \bmod 13 \\ &= 2^k \bmod 13 \end{aligned}$$

- Το 12 είναι η θεμελιώδης περίοδος, δεν υπάρχει μικρότερη από αυτή.

Συμπεριφορά g^x και $g^x \bmod p$ (3)

Για $g = 3$ και $p = 13$ έχουμε:

x	1	2	3	4	5	6	7	8	9	10	11
g^x	3	9	27	81	243	729	2187	6561	19683	59049	177147
$g^x \bmod p$	3	9	1	3	9	1	3	9	1	3	9

- Βλέπουμε ότι το $3^x \bmod 13$ δεν παίρνει όλες τις τιμές από το 1 μέχρι και το 12 πριν αρχίσει να επαναλαμβάνεται. Η θεμελιώδης περίοδός του είναι 3.
- Άρα αν έπρεπε να δοκιμάσουμε να βρούμε το x με $g = 3$ και $p = 13$ θα χρειαζόμασταν να δοκιμάσουμε μόνο 3 διαφορετικές τιμές.
- Γενικά θέλουμε τα g και p να είναι τέτοια που η περίοδος να είναι πολύ μεγάλη.

Επιλογή Παραμέτρων Diffie-Hellman

- Γενικώς επιλέγουμε τον p να είναι ένας μεγάλος πρώτος αριθμός.
- Αν αναπαρίσταται με 4096 bits, έχει τουλάχιστον 1233 δεκαδικά ψηφία.
- Στη συνέχεια επιλέγουμε ένα g σύμφωνα με τις αρχές της θεωρίας αριθμών ώστε η περίοδος του $g^x \bmod p$ να είναι πολύ μεγάλη.

Ιστορία

- Παρά το ότι η ανταλλαγή κλειδιών που περιγράψαμε παρουσιάστηκε από τους Diffie και Hellman, στην πραγματικότητα δεν ήταν οι πρώτοι που την ανακάλυψαν.
- Ο Malcolm John Williamson, ένας Βρετανός μαθηματικός και κρυπτογράφος, την είχε ανακαλύψει δύο χρόνια πριν από αυτούς, το 1974.
- Ο Williamson εργαζόταν στην Government Communications Headquarters (GCHQ), τη βρετανική υπηρεσία πληροφοριών και επικοινωνιών.
- Ως εκ τούτου δεν μπορούσε να δημοσιεύσει την ανακάλυψή του. Έγινε γνωστή πολύ αργότερα, το 1997.

Επισκόπηση

Γενικά

- Η ύψωση σε δύναμη είναι μια πράξη που απαιτείται συχνά στην κρυπτογραφία.
- Ο κλασικός τρόπος για να υπολογίζουμε το g^x απαιτεί x πολλαπλασιασμούς.
- Υπάρχει καλύτερος τρόπος;

Γρήγορη Ύψωση σε Δύναμη (1)

- Έστω ότι θέλουμε να υπολογίσουμε το g^x.
- Γράφουμε το x σε δυαδική μορφή:

$$x = b_{n-1}2^{n-1} + b_{n-2}2^{n-2} + \cdots + b_0 2^0$$

- Αυτό σημαίνει ότι:

$$g^x = g^{b_{n-1}2^{n-1}+b_{n-2}2^{n-2}+\cdots+b_0 2^0}$$

- Το οποίο είναι ισοδύναμο με:

$$g^x = (g^{2^{n-1}})^{b_{n-1}} \times (g^{2^{n-2}})^{b_{n-2}} \times \cdots \times (g^{2^0})^{b_0}$$

Γρήγορη Ύψωση σε Δύναμη (2)

- Για παράδειγμα, έστω ότι θέλουμε να υπολογίσουμε το 13^{13}.
- Το 13 στο δυαδικό σύστημα είναι 1101.
- Αυτό σημαίνει ότι το 13 γράφεται:

$$13 = 1 \times 2^3 + 1 \times 2^2 + 0 \times 2^1 + 1 \times 2^0$$

- Επομένως:

$$\begin{aligned} 13^{13} &= 13^{1\times 2^3 + 1\times 2^2 + 0\times 2^1 + 1\times 2^0} \\ &= (13^{2^3})^1 \times (13^{2^2})^1 \times (13^{2^1})^0 \times (13^{2^0})^1 \end{aligned}$$

Γρήγορη Ύψωση σε Δύναμη (3)

- Αν πάρουμε την τελευταία παράσταση από τα δεξιά προς τα αριστερά, ξεκινάμε υπολογίζοντας το $(g^{2^0})^{b_0}$.
- Μετά υπολογίζουμε τα:

$$(g^{2^1})^{b_1}$$

$$(g^{2^2})^{b_2}$$

$$(g^{2^3})^{b_3}$$

κ.λπ.

Γρήγορη Ύψωση σε Δύναμη (4)

- Αλλά:
  $g^{2^0} = g^1 = g$
  g^{2^1} είναι το τετράγωνο του g
  g^{2^2} είναι το τετράγωνο του g^{2^1}
  g^{2^3} είναι το τετράγωνο του g^{2^2}
  και γενικά $g^{2^k} = (g^{2^{k-1}})^2$ αφού $(g^{2^{k-1}})^2 = g^{2 \cdot 2^{k-1}}$.
- Συνεπώς μπορούμε να υπολογίσουμε το g^{2^i} για $i = 1, \ldots, n-1$, από τα δεξιά προς τα αριστερά υψώνοντας στο τετράγωνο τον αντίστοιχο προηγούμενο παράγοντα.
- Αυτό υλοποιείται με τον *αλγόριθμο ύψωσης σε δύναμη με επαναλαμβόμενο τετραγωνισμό* (exponentiation with repeated squaring).
- Ο αλγόριθμος αυτός έχει πολυπλοκότητα όσα τα bits του εκθέτη x, άρα $O(\lg x)$.

Ύψωση σε Δύναμη με Επαναλαμβόμενο Τετραγωνισμό

Algorithm: Exponentiation by repeated squaring.

`ExpRepeatedSquaring`$(g, x) \to r$

Input: g, the integer base
x, the integer exponent

Output: r, equal to g^x

```
1  c ← g
2  d ← x
3  r ← 1
4  while d > 0 do
5      if d mod 2 = 1 then
6          r ← r × c
7      d ← ⌊d/2⌋
8      c ← c × c
9  return r
```

Παράδειγμα Εκτέλεσης για 13^{13} (1)

$$
\begin{array}{c|cccccccc}
 & \multicolumn{7}{c}{\overbrace{\qquad\qquad\qquad\qquad\qquad\qquad\qquad}^{d}} & \\
c & 1 & & 1 & & 0 & & 1 & \\
\hline
13^{2^0} & & & & & & & (13^{2^0})^1 & \Big\} \\
13^{2^1} & & & & & (13^{2^1})^0 & \times & (13^{2^0})^1 & \\
13^{2^2} & & & (13^{2^2})^1 & \times & (13^{2^1})^0 & \times & (13^{2^0})^1 & r \\
13^{2^3} & (13^{2^3})^1 & \times & (13^{2^2})^1 & \times & (13^{2^1})^0 & \times & (13^{2^0})^1 & \Big\}
\end{array}
$$

Παράδειγμα Εκτέλεσης για 13^{13} (2)

$c = g^{2^i} = 13^{2^i}$	r	d
13	1	1101
169	13	110
28561	13	11
815730721	371293	1
	302875106592253	

- Κάθε γραμμή, εκτός από την τελευταία, αντιστοιχεί στις τιμές των c, r, και d, στη γραμμή 5 του αλγορίθμου.

Λεπτομέρειες Υλοποίησης (1)

- Για να βρούμε αν ένας ακέραιος αριθμός έχει υπόλοιπο 1 στη διαίρεση με το 2, όπως στη γραμμή 5 του αλγορίθμου, δεν χρειάζεται να κάνουμε διαίρεση.
- Αρκεί απλώς να ελέγξουμε αν το τελευταίο bit είναι 1.
- Αυτό μπορούμε να το κάνουμε απλά με τη δυαδική πράξη AND (συμβολίζεται με &), χρησιμοποιώντας έναν αριθμό που όλα τα bits του είναι 0, εκτός από το τελευταίο που είναι 1.
- Για παράδειγμα, για να ελέγξουμε το 13, κάνουμε:

$$1101\&0001 = 0001$$

Λεπτομέρειες Υλοποίησης (2)

- Ομοίως, για να κάνουμε ακέραια διαίρεση με το 2, όπως στη γραμμή 7 του αλγορίθμου, δεν χρειάζεται να κάνουμε την πράξη της διαίρεσης.
- Αρκεί απλώς να ολισθήσουμε τα bits του αριθμού μία θέση προς τα δεξιά.
- Αυτή η πράξη, *δεξιά ολίσθηση* (shift right), συμβολίζεται με $\gg$.
- Για παράδειγμα, για το 13, κάνουμε:

$$1101 \gg 1 = 110$$

Ύψωση σε Δύναμη με Υπόλοιπο με Επαναλαμβόμενο Τετραγωνισμό

- Από τον αλγόριθμο γρήγορης ύψωσης σε δύναμη φτάνουμε αμέσως στον αλγόριθμο ύψωσης σε δύναμη με υπόλοιπο, απλά εφαρμόζοντας την πράξη του υπολοίπου όπου χρειάζεται.
- Ο αλγόριθμος αυτός έχει επίσης πολυπλοκότητα όσα τα bits του εκθέτη x, άρα $O(\lg x)$.

Αλγόριθμος Ύψωσης σε Δύναμη με Υπόλοιπο με Επαναλαμβόμενο Τετραγωνισμό

Algorithm: Modular exponentiation by repeated squaring.

`ModExpRepeatedSquaring`$(g, x, p) \rightarrow r$

Input: g, the integer base
x, the integer exponent
p, the divisor

Output: r, equal to $g^x \bmod p$

```
1  c ← g mod p
2  d ← x
3  r ← 1
4  while d > 0 do
5      if d mod 2 = 1 then
6          r ← (r × c) mod p
7      d ← ⌊d/2⌋
8      c ← (c × c) mod p
9  return r
```

Παράδειγμα Εκτέλεσης για $155^{235} \bmod 391$

$c = g^{2^i} = 155^{2^i} \bmod 391$	r	d
155	1	11101011
174	155	1110101
169	382	111010
18	382	11101
324	229	1110
188	229	111
154	42	11
256	212	1
	314	