Classical Cryptography

Polyalphabetic substitution

Karst Koymans

Informatics Institute

University of Amsterdam

(version 22.5, 2023/02/14 13:15:31 UTC)

Tuesday, February 14, 2023

1. Early polyalphabetic systems
2. Later polyalphabetic systems
3. Variations
   - Porta
   - Some more options
4. A few related systems

Outline

Polyalphabetic ciphers

- Use more than one (cipher) alphabet
- Use a changing cipher alphabet (often for each plaintext letter)
- Leon Battista **Alberti** (1404 – 1472)
  - Cipher disk
- Johannes **Trithemius** (1462 – 1516)
  - Tabula recta
- Giovan Battista **Bellaso** (1505 – ca 1575)
  - Keyed polyalphabetic cipher
- Giambattista della **Porta** (ca 1535 – 1615)
  - Porta reduced table

Alberti

Figure 1: Leon Battista Alberti (1404 – 1472)

Source: https://en.wikipedia.org/wiki/Leon_Battista_Alberti

Leon Battista Alberti (1404 – 1472)

- *De Cifris* (On Ciphers)
- Cipher disk
- Regularly change the cipher alphabet
- Communicate a change in ciphertext
- The outer ring is used for plaintext
- The inner ring is used for ciphertext

Trithemius

Figure 2: Johannes Trithemius (1462 – 1516)

Source: https://en.wikipedia.org/wiki/Johannes_Trithemius

Johannes Trithemius (1462 – 1516)

- Tabula recta
  - “proper table”
  - square table
  - letter square
  - tableau
- Progressive system
  - The cipher alphabet changes each letter by taking the next line in the tabula recta

Tabula recta

	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	X	Y	Z	W
0	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	X	Y	Z	W
1	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	X	Y	Z	W	A
2	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	X	Y	Z	W	A	B
3	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	X	Y	Z	W	A	B	C
4	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	X	Y	Z	W	A	B	C	D
5	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	X	Y	Z	W	A	B	C	D	E
6	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	X	Y	Z	W	A	B	C	D	E	F
7	H	I	K	L	M	N	O	P	Q	R	S	T	U	X	Y	Z	W	A	B	C	D	E	F	G
8	I	K	L	M	N	O	P	Q	R	S	T	U	X	Y	Z	W	A	B	C	D	E	F	G	H
9	K	L	M	N	O	P	Q	R	S	T	U	X	Y	Z	W	A	B	C	D	E	F	G	H	I
10	L	M	N	O	P	Q	R	S	T	U	X	Y	Z	W	A	B	C	D	E	F	G	H	I	K
11	M	N	O	P	Q	R	S	T	U	X	Y	Z	W	A	B	C	D	E	F	G	H	I	K	L
12	N	O	P	Q	R	S	T	U	X	Y	Z	W	A	B	C	D	E	F	G	H	I	K	L	M
13	O	P	Q	R	S	T	U	X	Y	Z	W	A	B	C	D	E	F	G	H	I	K	L	M	N
14	P	Q	R	S	T	U	X	Y	Z	W	A	B	C	D	E	F	G	H	I	K	L	M	N	O
15	Q	R	S	T	U	X	Y	Z	W	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P
16	R	S	T	U	X	Y	Z	W	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q
17	S	T	U	X	Y	Z	W	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R
18	T	U	X	Y	Z	W	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S
19	U	X	Y	Z	W	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T
20	X	Y	Z	W	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U
21	Y	Z	W	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	X
22	Z	W	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	X	Y
23	W	A	B	C	D	E	F	G	H	I	K	L	M	N	O	P	Q	R	S	T	U	X	Y	Z

Figure 3: Original tabula recta (no J, V; W at end)

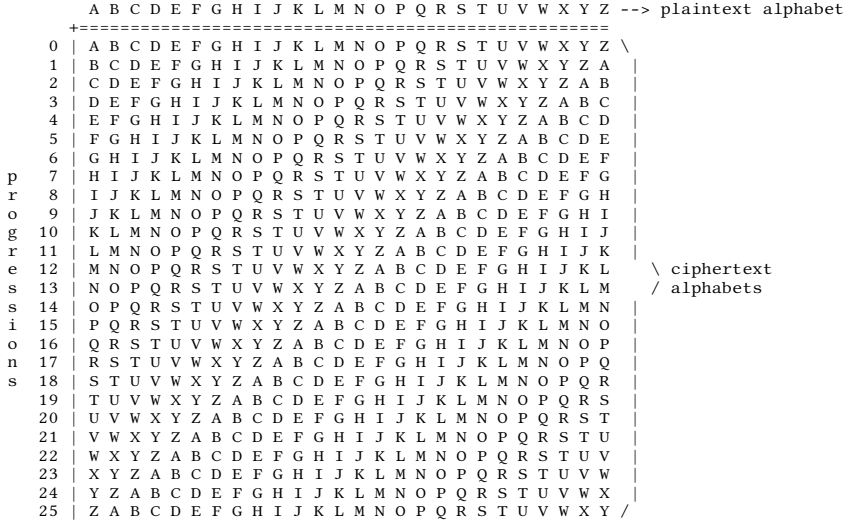


Figure 4: Modern (progressive) tabula recta

Periodic progressive systems

- Normal progression $0, 1, 2, \ldots$ is very regular
  - Its period is 26
- To make things less predictable you can vary the progression
  - A step pattern like $1, 3, 2$ generates the irregular progression $0, 1, 4, 6, 7, 10, 12, \ldots$
  - The progression index (PGI) is $1 + 3 + 2 = 6$ and the progression length (L) is 3
  - Now the period turns out to be $\frac{\mathrm{lcm}(\mathrm{PGI}, 26)}{\mathrm{PGI}} \cdot \mathrm{L} = \frac{\mathrm{lcm}(6, 26)}{6} \cdot 3 = 39$
  - The general formula for an alphabet of size N is $\frac{\mathrm{lcm}(\mathrm{PGI}, \mathrm{N})}{\mathrm{PGI}} \cdot \mathrm{L} = \frac{\mathrm{N}}{\gcd(\mathrm{PGI}, \mathrm{N})} \cdot \mathrm{L}$

Kryha encryption device

- Mechanical device making irregular steps when pushing a lever
  - With 17-steps pattern $7, 6, 7, 5, 6, 7, 6, 8, 6, 10, 5, 6, 5, 7, 6, 5, 9$
  - The period is an impressive $17 \cdot 26 = 442$

Kryha cryptanalysis

- Cryptanalysis by William Friedman and his team
  - William Friedman, Solomon Kullback, Frank Rowlett and Abraham Sinkov
- The challenge given was a 1135 letter cryptogram
- The challenge was broken – without computers – in a mere 2 hours and 41 minutes

Giovan Battista Bellaso (1505 – ca 1575)

- “Forgotten by history”
- Introduced the keyed polyalphabet
  - Repeating-key cipher
  - Later named after Blaise de **Vigenère**
- Used reciprocal alphabets
  - Makes encryption and decryption identical operations
  - Later named after Francis **Beaufort**

Outline

Vigenère

Figure 5: Blaise de Vigenère (1523 – 1596)

Source: https://en.wikipedia.org/wiki/Blaise_de_Vigenère

Blaise de Vigenère (1523 – 1596)

- Used Bellaso's ideas
- Combined the following ideas
  - Tabula recta (now called Vigenère square)
  - Repeating-key cipher
- Plaintext letters are along the top of the diagram
- Ciphertext letters inside the table
- Key letters are along the left side of the diagram
  - A key letter equals the first letter of the cipher alphabet

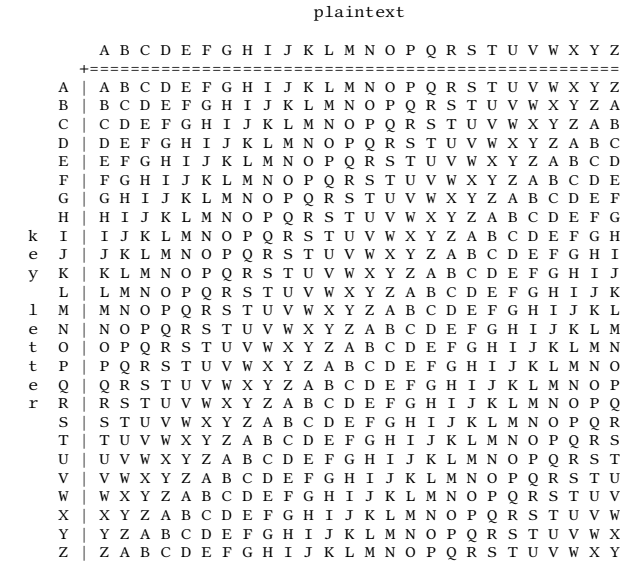


Figure 6: Vigenère table (modern encoding)

Mathematical formulation of Vigenère's encryption

- Let $P = P_0 P_1 \dots P_{n-1}$ be the plaintext
- Let $K = K_0 K_1 \dots K_{p-1}$ be the key with **period p**
- Then the cryptogram $C = C_0 C_1 \dots C_{n-1}$ is given by
  - $C_i = \mathcal{E}_i(P_i) = P_i + K_{i \pmod p} \pmod{26}$
- For decryption we conclude
  - $P_i = \mathcal{D}_i(C_i) = C_i - K_{i \pmod p} \pmod{26}$
- Exchanging encryption and decryption is called "Variant Vigenère"

More room for confusion

- Assume we want to keep the simple mathematical relationship between plaintext letter and cryptogram letter: $C = P + K$
- Also assume we want to use legacy encoding
- The only way this works is by using an **alternative** Vigenère
- This non-standard table is what is used in “The Mathematics of Secrets”
- In this case the key letters are not the first elements of the cipher alphabet

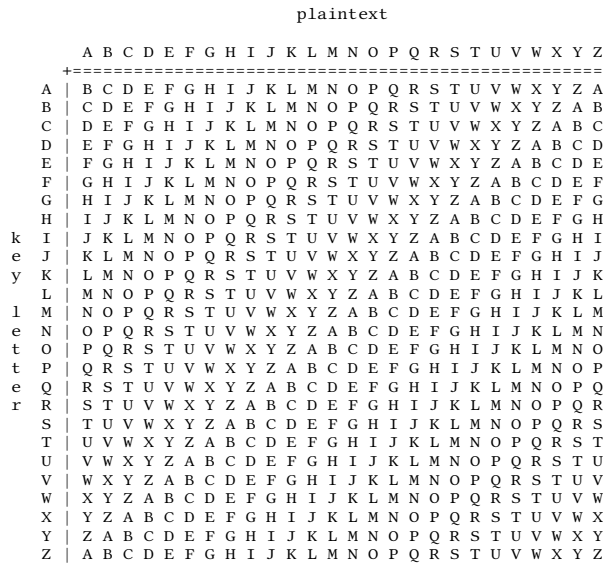


Figure 7: Alternative Vigenère table (legacy encoding; used in book)

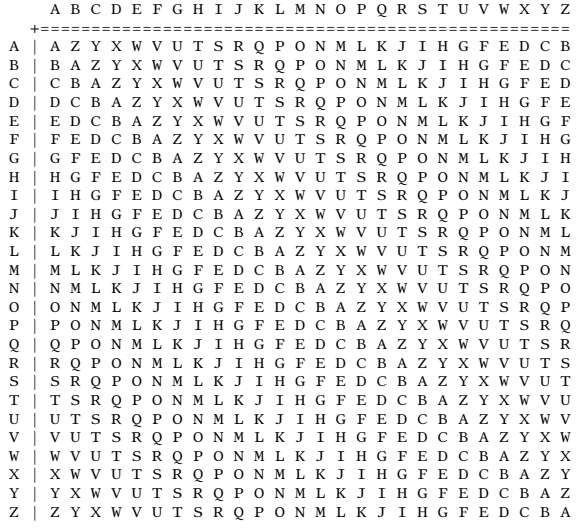
Beaufort

Figure 8: Francis Beaufort (1774 – 1857)

Source: https://en.wikipedia.org/wiki/Francis_Beaufort

Francis Beaufort (1774 – 1857)

- Changes Vigenère square by starting with a mixed cipher alphabet
  - Which is a Caesar (key = 1) shift of the atbash cipher
  - Or if you want the atbash of a Caesar (key = -1) shift
- In modern encoding the Beaufort starting cipher alphabetcan also be described simply as a multiplicative cipher with factor -1
- In legacy encoding the Beaufort starting cipher alphabet
  - must be described by a more complicated affine cipher with
    - factor -1
    - additive 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	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B
B	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C
C	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D
D	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E
E	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F
F	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G
G	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H
H	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I
I	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J
J	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K
K	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L
L	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M
M	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O	N
N	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P	O
O	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q	P
P	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R	Q
Q	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S	R
R	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T	S
S	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U	T
T	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V	U
U	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W	V
V	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X	W
W	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y	X
X	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z	Y
Y	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z
Z	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A

Figure 9: Beaufort table

Mathematical formulation of Beaufort's encryption

- Let $P = P_0 P_1 \dots P_{n-1}$ be the plaintext (in modern encoding)
- Let $K = K_0 K_1 \dots K_{p-1}$ be the key with **period p**
- Then the cryptogram $C = C_0 C_1 \dots C_{n-1}$ is given by
  - $C_i = \mathcal{E}_i(P_i) = -P_i + K_{i \pmod p} \pmod{26}$
- For decryption we conclude
  - $P_i = \mathcal{D}_i(C_i) = -C_i + K_{i \pmod p} \pmod{26}$
- Now we clearly see the symmetric role of encryption and decryption
  - $P_i + C_i = C_i + P_i = K_{i \pmod p} \pmod{26}$

Outline

Outline

della Porta

Figure 10: Giambattista della Porta (ca 1535 – 1615)

Source: https://en.wikipedia.org/wiki/Giambattista_della_Porta

Giambattista della Porta (ca 1535 – 1615)

- Introduced the first digraph substitution
  - *De furtivis Literarum Notis* (1563)
    - His scientific work on cryptography
- Introduced another polyalphabetic cipher based on a reduced size table
  - Porta's reduced 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	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
B	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
C	O	P	Q	R	S	T	U	V	W	X	Y	Z	N	M	A	B	C	D	E	F	G	H	I	J	K	L
D	O	P	Q	R	S	T	U	V	W	X	Y	Z	N	M	A	B	C	D	E	F	G	H	I	J	K	L
E	P	Q	R	S	T	U	V	W	X	Y	Z	N	O	L	M	A	B	C	D	E	F	G	H	I	J	K
F	P	Q	R	S	T	U	V	W	X	Y	Z	N	O	L	M	A	B	C	D	E	F	G	H	I	J	K
G	Q	R	S	T	U	V	W	X	Y	Z	N	O	P	K	L	M	A	B	C	D	E	F	G	H	I	J
H	Q	R	S	T	U	V	W	X	Y	Z	N	O	P	K	L	M	A	B	C	D	E	F	G	H	I	J
I	R	S	T	U	V	W	X	Y	Z	N	O	P	Q	J	K	L	M	A	B	C	D	E	F	G	H	I
J	R	S	T	U	V	W	X	Y	Z	N	O	P	Q	J	K	L	M	A	B	C	D	E	F	G	H	I
K	S	T	U	V	W	X	Y	Z	N	O	P	Q	R	I	J	K	L	M	A	B	C	D	E	F	G	H
L	S	T	U	V	W	X	Y	Z	N	O	P	Q	R	I	J	K	L	M	A	B	C	D	E	F	G	H
M	T	U	V	W	X	Y	Z	N	O	P	Q	R	S	H	I	J	K	L	M	A	B	C	D	E	F	G
N	T	U	V	W	X	Y	Z	N	O	P	Q	R	S	H	I	J	K	L	M	A	B	C	D	E	F	G
O	U	V	W	X	Y	Z	N	O	P	Q	R	S	T	G	H	I	J	K	L	M	A	B	C	D	E	F
P	U	V	W	X	Y	Z	N	O	P	Q	R	S	T	G	H	I	J	K	L	M	A	B	C	D	E	F
Q	V	W	X	Y	Z	N	O	P	Q	R	S	T	U	F	G	H	I	J	K	L	M	A	B	C	D	E
R	V	W	X	Y	Z	N	O	P	Q	R	S	T	U	F	G	H	I	J	K	L	M	A	B	C	D	E
S	W	X	Y	Z	N	O	P	Q	R	S	T	U	V	E	F	G	H	I	J	K	L	M	A	B	C	D
T	W	X	Y	Z	N	O	P	Q	R	S	T	U	V	E	F	G	H	I	J	K	L	M	A	B	C	D
U	X	Y	Z	N	O	P	Q	R	S	T	U	V	W	D	E	F	G	H	I	J	K	L	M	A	B	C
V	X	Y	Z	N	O	P	Q	R	S	T	U	V	W	D	E	F	G	H	I	J	K	L	M	A	B	C
W	Y	Z	N	O	P	Q	R	S	T	U	V	W	X	C	D	E	F	G	H	I	J	K	L	M	A	B
X	Y	Z	N	O	P	Q	R	S	T	U	V	W	X	C	D	E	F	G	H	I	J	K	L	M	A	B
Y	Z	N	O	P	Q	R	S	T	U	V	W	X	Y	B	C	D	E	F	G	H	I	J	K	L	M	A
Z	Z	N	O	P	Q	R	S	T	U	V	W	X	Y	B	C	D	E	F	G	H	I	J	K	L	M	A

Figure 11: Full Porta table

Reduced Porta table

	A	B	C	D	E	F	G	H	I	J	K	L	M
AB	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
CD	O	P	Q	R	S	T	U	V	W	X	Y	Z	N
EF	P	Q	R	S	T	U	V	W	X	Y	Z	N	O
GH	Q	R	S	T	U	V	W	X	Y	Z	N	O	P
IJ	R	S	T	U	V	W	X	Y	Z	N	O	P	Q
KL	S	T	U	V	W	X	Y	Z	N	O	P	Q	R
MN	T	U	V	W	X	Y	Z	N	O	P	Q	R	S
OP	U	V	W	X	Y	Z	N	O	P	Q	R	S	T
QR	V	W	X	Y	Z	N	O	P	Q	R	S	T	U
ST	W	X	Y	Z	N	O	P	Q	R	S	T	U	V
UV	X	Y	Z	N	O	P	Q	R	S	T	U	V	W
WX	Y	Z	N	O	P	Q	R	S	T	U	V	W	X
YZ	Z	N	O	P	Q	R	S	T	U	V	W	X	Y

Figure 12: Reduced Porta table

Outline

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

Figure 13: “Plain mixed up”-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	C	I	P	H	E	R	M	X	D	U	A	B	F	G	J	K	L	N	O	Q	S	T	V	W	Y	Z
B	I	P	H	E	R	M	X	D	U	A	B	F	G	J	K	L	N	O	Q	S	T	V	W	Y	Z	C
C	P	H	E	R	M	X	D	U	A	B	F	G	J	K	L	N	O	Q	S	T	V	W	Y	Z	C	I
D	H	E	R	M	X	D	U	A	B	F	G	J	K	L	N	O	Q	S	T	V	W	Y	Z	C	I	P
E	E	R	M	X	D	U	A	B	F	G	J	K	L	N	O	Q	S	T	V	W	Y	Z	C	I	P	H
F	R	M	X	D	U	A	B	F	G	J	K	L	N	O	Q	S	T	V	W	Y	Z	C	I	P	H	E
G	M	X	D	U	A	B	F	G	J	K	L	N	O	Q	S	T	V	W	Y	Z	C	I	P	H	E	R
H	X	D	U	A	B	F	G	J	K	L	N	O	Q	S	T	V	W	Y	Z	C	I	P	H	E	R	M
I	D	U	A	B	F	G	J	K	L	N	O	Q	S	T	V	W	Y	Z	C	I	P	H	E	R	M	X
J	U	A	B	F	G	J	K	L	N	O	Q	S	T	V	W	Y	Z	C	I	P	H	E	R	M	X	D
K	A	B	F	G	J	K	L	N	O	Q	S	T	V	W	Y	Z	C	I	P	H	E	R	M	X	D	U
L	B	F	G	J	K	L	N	O	Q	S	T	V	W	Y	Z	C	I	P	H	E	R	M	X	D	U	A
M	F	G	J	K	L	N	O	Q	S	T	V	W	Y	Z	C	I	P	H	E	R	M	X	D	U	A	B
N	G	J	K	L	N	O	Q	S	T	V	W	Y	Z	C	I	P	H	E	R	M	X	D	U	A	B	F
O	J	K	L	N	O	Q	S	T	V	W	Y	Z	C	I	P	H	E	R	M	X	D	U	A	B	F	G
P	K	L	N	O	Q	S	T	V	W	Y	Z	C	I	P	H	E	R	M	X	D	U	A	B	F	G	J
Q	L	N	O	Q	S	T	V	W	Y	Z	C	I	P	H	E	R	M	X	D	U	A	B	F	G	J	K
R	N	O	Q	S	T	V	W	Y	Z	C	I	P	H	E	R	M	X	D	U	A	B	F	G	J	K	L
S	O	Q	S	T	V	W	Y	Z	C	I	P	H	E	R	M	X	D	U	A	B	F	G	J	K	L	N
T	Q	S	T	V	W	Y	Z	C	I	P	H	E	R	M	X	D	U	A	B	F	G	J	K	L	N	O
U	S	T	V	W	Y	Z	C	I	P	H	E	R	M	X	D	U	A	B	F	G	J	K	L	N	O	Q
V	T	V	W	Y	Z	C	I	P	H	E	R	M	X	D	U	A	B	F	G	J	K	L	N	O	Q	S
W	V	W	Y	Z	C	I	P	H	E	R	M	X	D	U	A	B	F	G	J	K	L	N	O	Q	S	T
X	W	Y	Z	C	I	P	H	E	R	M	X	D	U	A	B	F	G	J	K	L	N	O	Q	S	T	V
Y	Y	Z	C	I	P	H	E	R	M	X	D	U	A	B	F	G	J	K	L	N	O	Q	S	T	V	W
Z	Z	C	I	P	H	E	R	M	X	D	U	A	B	F	G	J	K	L	N	O	Q	S	T	V	W	Y

Figure 14: “Cipher mixed up”-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
C	C	I	P	H	E	R	M	X	D	U	A	B	F	G	J	K	L	N	O	Q	S	T	V	W	Y	Z
I	I	P	H	E	R	M	X	D	U	A	B	F	G	J	K	L	N	O	Q	S	T	V	W	Y	Z	C
P	P	H	E	R	M	X	D	U	A	B	F	G	J	K	L	N	O	Q	S	T	V	W	Y	Z	C	I
H	H	E	R	M	X	D	U	A	B	F	G	J	K	L	N	O	Q	S	T	V	W	Y	Z	C	I	P
E	E	R	M	X	D	U	A	B	F	G	J	K	L	N	O	Q	S	T	V	W	Y	Z	C	I	P	H
R	R	M	X	D	U	A	B	F	G	J	K	L	N	O	Q	S	T	V	W	Y	Z	C	I	P	H	E
M	M	X	D	U	A	B	F	G	J	K	L	N	O	Q	S	T	V	W	Y	Z	C	I	P	H	E	R
X	X	D	U	A	B	F	G	J	K	L	N	O	Q	S	T	V	W	Y	Z	C	I	P	H	E	R	M
D	D	U	A	B	F	G	J	K	L	N	O	Q	S	T	V	W	Y	Z	C	I	P	H	E	R	M	X
U	U	A	B	F	G	J	K	L	N	O	Q	S	T	V	W	Y	Z	C	I	P	H	E	R	M	X	D
A	A	B	F	G	J	K	L	N	O	Q	S	T	V	W	Y	Z	C	I	P	H	E	R	M	X	D	U
B	B	F	G	J	K	L	N	O	Q	S	T	V	W	Y	Z	C	I	P	H	E	R	M	X	D	U	A
F	F	G	J	K	L	N	O	Q	S	T	V	W	Y	Z	C	I	P	H	E	R	M	X	D	U	A	B
G	G	J	K	L	N	O	Q	S	T	V	W	Y	Z	C	I	P	H	E	R	M	X	D	U	A	B	F
J	J	K	L	N	O	Q	S	T	V	W	Y	Z	C	I	P	H	E	R	M	X	D	U	A	B	F	G
K	K	L	N	O	Q	S	T	V	W	Y	Z	C	I	P	H	E	R	M	X	D	U	A	B	F	G	J
L	L	N	O	Q	S	T	V	W	Y	Z	C	I	P	H	E	R	M	X	D	U	A	B	F	G	J	K
N	N	O	Q	S	T	V	W	Y	Z	C	I	P	H	E	R	M	X	D	U	A	B	F	G	J	K	L
O	O	Q	S	T	V	W	Y	Z	C	I	P	H	E	R	M	X	D	U	A	B	F	G	J	K	L	N
Q	Q	S	T	V	W	Y	Z	C	I	P	H	E	R	M	X	D	U	A	B	F	G	J	K	L	N	O
S	S	T	V	W	Y	Z	C	I	P	H	E	R	M	X	D	U	A	B	F	G	J	K	L	N	O	Q
T	T	V	W	Y	Z	C	I	P	H	E	R	M	X	D	U	A	B	F	G	J	K	L	N	O	Q	S
V	V	W	Y	Z	C	I	P	H	E	R	M	X	D	U	A	B	F	G	J	K	L	N	O	Q	S	T
W	W	Y	Z	C	I	P	H	E	R	M	X	D	U	A	B	F	G	J	K	L	N	O	Q	S	T	V
Y	Y	Z	C	I	P	H	E	R	M	X	D	U	A	B	F	G	J	K	L	N	O	Q	S	T	V	W
Z	Z	C	I	P	H	E	R	M	X	D	U	A	B	F	G	J	K	L	N	O	Q	S	T	V	W	Y

Figure 15: “Cipher and key mixed up”-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	A	B	F	G	J	K	L	N	O	Q	S	T	V	W	Y	Z	C	I	P	H	E	R	M	X	D	U
B	B	F	G	J	K	L	N	O	Q	S	T	V	W	Y	Z	C	I	P	H	E	R	M	X	D	U	A
C	C	I	P	H	E	R	M	X	D	U	A	B	F	G	J	K	L	N	O	Q	S	T	V	W	Y	Z
D	D	U	A	B	F	G	J	K	L	N	O	Q	S	T	V	W	Y	Z	C	I	P	H	E	R	M	X
E	E	R	M	X	D	U	A	B	F	G	J	K	L	N	O	Q	S	T	V	W	Y	Z	C	I	P	H
F	F	G	J	K	L	N	O	Q	S	T	V	W	Y	Z	C	I	P	H	E	R	M	X	D	U	A	B
G	G	J	K	L	N	O	Q	S	T	V	W	Y	Z	C	I	P	H	E	R	M	X	D	U	A	B	F
H	H	E	R	M	X	D	U	A	B	F	G	J	K	L	N	O	Q	S	T	V	W	Y	Z	C	I	P
I	I	P	H	E	R	M	X	D	U	A	B	F	G	J	K	L	N	O	Q	S	T	V	W	Y	Z	C
J	J	K	L	N	O	Q	S	T	V	W	Y	Z	C	I	P	H	E	R	M	X	D	U	A	B	F	G
K	K	L	N	O	Q	S	T	V	W	Y	Z	C	I	P	H	E	R	M	X	D	U	A	B	F	G	J
L	L	N	O	Q	S	T	V	W	Y	Z	C	I	P	H	E	R	M	X	D	U	A	B	F	G	J	K
M	M	X	D	U	A	B	F	G	J	K	L	N	O	Q	S	T	V	W	Y	Z	C	I	P	H	E	R
N	N	O	Q	S	T	V	W	Y	Z	C	I	P	H	E	R	M	X	D	U	A	B	F	G	J	K	L
O	O	Q	S	T	V	W	Y	Z	C	I	P	H	E	R	M	X	D	U	A	B	F	G	J	K	L	N
P	P	H	E	R	M	X	D	U	A	B	F	G	J	K	L	N	O	Q	S	T	V	W	Y	Z	C	I
Q	Q	S	T	V	W	Y	Z	C	I	P	H	E	R	M	X	D	U	A	B	F	G	J	K	L	N	O
R	R	M	X	D	U	A	B	F	G	J	K	L	N	O	Q	S	T	V	W	Y	Z	C	I	P	H	E
S	S	T	V	W	Y	Z	C	I	P	H	E	R	M	X	D	U	A	B	F	G	J	K	L	N	O	Q
T	T	V	W	Y	Z	C	I	P	H	E	R	M	X	D	U	A	B	F	G	J	K	L	N	O	Q	S
U	U	A	B	F	G	J	K	L	N	O	Q	S	T	V	W	Y	Z	C	I	P	H	E	R	M	X	D
V	V	W	Y	Z	C	I	P	H	E	R	M	X	D	U	A	B	F	G	J	K	L	N	O	Q	S	T
W	W	Y	Z	C	I	P	H	E	R	M	X	D	U	A	B	F	G	J	K	L	N	O	Q	S	T	V
X	X	D	U	A	B	F	G	J	K	L	N	O	Q	S	T	V	W	Y	Z	C	I	P	H	E	R	M
Y	Y	Z	C	I	P	H	E	R	M	X	D	U	A	B	F	G	J	K	L	N	O	Q	S	T	V	W
Z	Z	C	I	P	H	E	R	M	X	D	U	A	B	F	G	J	K	L	N	O	Q	S	T	V	W	Y

Figure 16: “Cipher and key mixed up (sorted)”-table

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

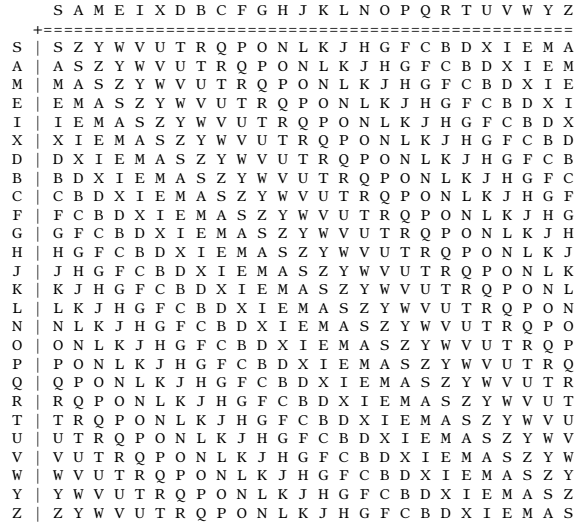
Figure 17: “Plain, cipher and key mixed up”-table

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

Figure 18: “Plain, cipher and key mixed up (sorted)”-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	B	Q	S	N	L	T	V	W	F	Y	Z	A	J	G	C	U	I	P	H	E	O	R	M	K	X	D
B	F	S	T	O	N	V	W	Y	G	Z	C	B	K	J	I	A	P	H	E	R	Q	M	X	L	D	U
C	G	T	V	Q	O	W	Y	Z	J	C	I	F	L	K	P	B	H	E	R	M	S	X	D	N	U	A
D	D	L	N	J	G	O	Q	S	U	T	V	X	B	A	W	M	Y	Z	C	I	K	P	H	F	E	R
E	H	B	F	U	D	G	J	K	E	L	N	P	M	R	O	I	Q	S	T	V	A	W	Y	X	Z	C
F	J	V	W	S	Q	Y	Z	C	K	I	P	G	N	L	H	F	E	R	M	X	T	D	U	O	A	B
G	K	W	Y	T	S	Z	C	I	L	P	H	J	O	N	E	G	R	M	X	D	V	U	A	Q	B	F
H	L	Y	Z	V	T	C	I	P	N	H	E	K	Q	O	R	J	M	X	D	U	W	A	B	S	F	G
I	M	J	K	F	B	L	N	O	X	Q	S	R	U	D	T	E	V	W	Y	Z	G	C	I	A	P	H
J	N	Z	C	W	V	I	P	H	O	E	R	L	S	Q	M	K	X	D	U	A	Y	B	F	T	G	J
K	P	A	B	D	X	F	G	J	H	K	L	I	R	E	N	C	O	Q	S	T	U	V	W	M	Y	Z
L	O	C	I	Y	W	P	H	E	Q	R	M	N	T	S	X	L	D	U	A	B	Z	F	G	V	J	K
M	R	G	J	B	A	K	L	N	M	O	Q	E	D	X	S	H	T	V	W	Y	F	Z	C	U	I	P
N	Q	I	P	Z	Y	H	E	R	S	M	X	O	V	T	D	N	U	A	B	F	C	G	J	W	K	L
O	S	P	H	C	Z	E	R	M	T	X	D	Q	W	V	U	O	A	B	F	G	I	J	K	Y	L	N
P	A	O	Q	L	K	S	T	V	B	W	Y	U	G	F	Z	D	C	I	P	H	N	E	R	J	M	X
Q	T	H	E	I	C	R	M	X	V	D	U	S	Y	W	A	Q	B	F	G	J	P	K	L	Z	N	O
R	V	E	R	P	I	M	X	D	W	U	A	T	Z	Y	B	S	F	G	J	K	H	L	N	C	O	Q
S	W	R	M	H	P	X	D	U	Y	A	B	V	C	Z	F	T	G	J	K	L	E	N	O	I	Q	S
T	Y	M	X	E	H	D	U	A	Z	B	F	W	I	C	G	V	J	K	L	N	R	O	Q	P	S	T
U	U	N	O	K	J	Q	S	T	A	V	W	D	F	B	Y	X	Z	C	I	P	L	H	E	G	R	M
V	Z	X	D	R	E	U	A	B	C	F	G	Y	P	I	J	W	K	L	N	O	M	Q	S	H	T	V
W	C	D	U	M	R	A	B	F	I	G	J	Z	H	P	K	Y	L	N	O	Q	X	S	T	E	V	W
X	X	K	L	G	F	N	O	Q	D	S	T	M	A	U	V	R	W	Y	Z	C	J	I	P	B	H	E
Y	E	F	G	A	U	J	K	L	R	N	O	H	X	M	Q	P	S	T	V	W	B	Y	Z	D	C	I
Z	I	U	A	X	M	B	F	G	P	J	K	C	E	H	L	Z	N	O	Q	S	D	T	V	R	W	Y

Figure 19: “Plain, cipher and key mixed up (all sorted)”-table



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

Figure 20: “Same mixed (Beaufort-style)” 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	S	T	R	U	Y	Q	P	O	W	N	L	K	Z	J	H	G	F	C	A	B	D	X	I	V	E	M
B	D	S	Z	A	I	Y	W	V	E	U	T	R	X	Q	P	O	N	L	B	K	J	H	G	M	F	C
C	B	A	S	M	X	Z	Y	W	I	V	U	T	D	R	Q	P	O	N	C	L	K	J	H	E	G	F
D	X	Z	Y	S	E	W	V	U	M	T	R	Q	I	P	O	N	L	K	D	J	H	G	F	A	C	B
E	M	V	U	W	S	T	R	Q	Z	P	O	N	A	L	K	J	H	G	E	F	C	B	D	Y	X	I
F	C	M	A	E	D	S	Z	Y	X	W	V	U	B	T	R	Q	P	O	F	N	L	K	J	I	H	G
G	F	E	M	I	B	A	S	Z	D	Y	W	V	C	U	T	R	Q	P	G	O	N	L	K	X	J	H
H	G	I	E	X	C	M	A	S	B	Z	Y	W	F	V	U	T	R	Q	H	P	O	N	L	D	K	J
I	E	W	V	Y	A	U	T	R	S	Q	P	O	M	N	L	K	J	H	I	G	F	C	B	Z	D	X
J	H	X	I	D	F	E	M	A	C	S	Z	Y	G	W	V	U	T	R	J	Q	P	O	N	B	L	K
K	J	D	X	B	G	I	E	M	F	A	S	Z	H	Y	W	V	U	T	K	R	Q	P	O	C	N	L
L	K	B	D	C	H	X	I	E	G	M	A	S	J	Z	Y	W	V	U	L	T	R	Q	P	F	O	N
M	A	U	T	V	Z	R	Q	P	Y	O	N	L	S	K	J	H	G	F	M	C	B	D	X	W	I	E
N	L	C	B	F	J	D	X	I	H	E	M	A	K	S	Z	Y	W	V	N	U	T	R	Q	G	P	O
O	N	F	C	G	K	B	D	X	J	I	E	M	L	A	S	Z	Y	W	O	V	U	T	R	H	Q	P
P	O	G	F	H	L	C	B	D	K	X	I	E	N	M	A	S	Z	Y	P	W	V	U	T	J	R	Q
Q	P	H	G	J	N	F	C	B	L	D	X	I	O	E	M	A	S	Z	Q	Y	W	V	U	K	T	R
R	Q	J	H	K	O	G	F	C	N	B	D	X	P	I	E	M	A	S	R	Z	Y	W	V	L	U	T
S	Z	R	Q	T	W	P	O	N	V	L	K	J	Y	H	G	F	C	B	S	D	X	I	E	U	M	A
T	R	K	J	L	P	H	G	F	O	C	B	D	Q	X	I	E	M	A	T	S	Z	Y	W	N	V	U
U	T	L	K	N	Q	J	H	G	P	F	C	B	R	D	X	I	E	M	U	A	S	Z	Y	O	W	V
V	U	N	L	O	R	K	J	H	Q	G	F	C	T	B	D	X	I	E	V	M	A	S	Z	P	Y	W
W	V	O	N	P	T	L	K	J	R	H	G	F	U	C	B	D	X	I	W	E	M	A	S	Q	Z	Y
X	I	Y	W	Z	M	V	U	T	A	R	Q	P	E	O	N	L	K	J	X	H	G	F	C	S	B	D
Y	W	P	O	Q	U	N	L	K	T	J	H	G	V	F	C	B	D	X	Y	I	E	M	A	R	S	Z
Z	Y	Q	P	R	V	O	N	L	U	K	J	H	W	G	F	C	B	D	Z	X	I	E	M	T	A	S

Figure 21: “Same mixed (Beaufort style and sorted)”-table

Outline

Multiplex systems (1): Alphabet strips

- Choose a set of alphabet strips from a given collection
- Each strip contains (two copies of) a permutation of the alphabet
- Put the plaintext inside one of the columns
- Read off the ciphertext from any other column
  - Each of the other 25 columns is called a **generatrix**

Alphabet strip example

```
                plain           crypto
                  v               w
11 A L T M S X V Q P N O H U W D I Z Y C G K R F B E J
 3 C Z I N X F Y Q R T V W L A D K O M J U B G E P H S
23 J C P G B Z A X K W R E V D T U F O Y H M L S I Q N
12 V E W O A M N F L H Q G C U J T B Y P Z K X I S R D
 7 V R O G S Y D U L C F M Q T W A H X J E Z B N I K P
      w         v
11 M S X V Q P N O H U W D I Z Y C G K R F B E J A L T
 3 Q R T V W L A D K O M J U B G E P H S C Z I N X F Y
23 X K W R E V D T U F O Y H M L S I Q N J C P G B Z A
12 X I S R D V E W O A M N F L H Q G C U J T B Y P Z K
 7 B N I K P V R O G S Y D U L C F M Q T W A H X J E Z
                  v       w
11 F B E J A L T M S X V Q P N O H U W D I Z Y C G K R
 3 F Y Q R T V W L A D K O M J U B G E P H S C Z I N X
23 J C P G B Z A X K W R E V D T U F O Y H M L S I Q N
12 H Q G C U J T B Y P Z K X I S R D V E W O A M N F L
 7 T W A H X J E Z B N I K P V R O G S Y D U L C F M Q
                  v               w
11 I Z Y C G K R F B E J A L T M S X V Q P N O H U W D
```

Figure 22: Encryption of VYAND NADERT WATER into DDTJW XTWSI VKRZI X

Source: Syllabus Hans van der Meer

Alphabet strips (M-138-A)

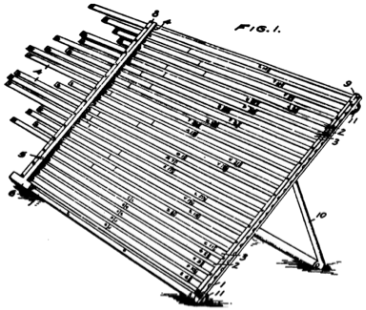
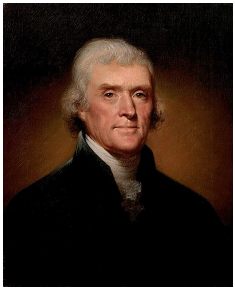


Figure 23: William Friedman's alphabet strips device

Source: Syllabus Hans van der Meer

Jefferson and Bazeries



Thomas Jefferson

Étienne Bazeries

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

http://www.bibmath.net/crypto/complements/images/bazeries.jpg

Multiplex systems (2): Jefferson disk (M-94)

- This is based on the same idea as the alphabet strips
- The alphabets are circumscribed on wheels mounted on a cylinder
- It is also called a Bazeries cylinder

Source: Syllabus Hans van der Meer

Rotor based systems

- Similar to a progressive system based on a mixed cipher alphabet
- The difference is that it also has a “regressive” component
- In fact the next cipher alphabet is a **conjugation**

  of the current cipher alphabet with a “Caesar 1” cipher
- Let R be the (arbitrary) rotor permutation and C an additive permutation with addition 1
- Then after k rotation steps the permutation is given by

$$R_k = C^{-k} \circ R \circ C^k$$