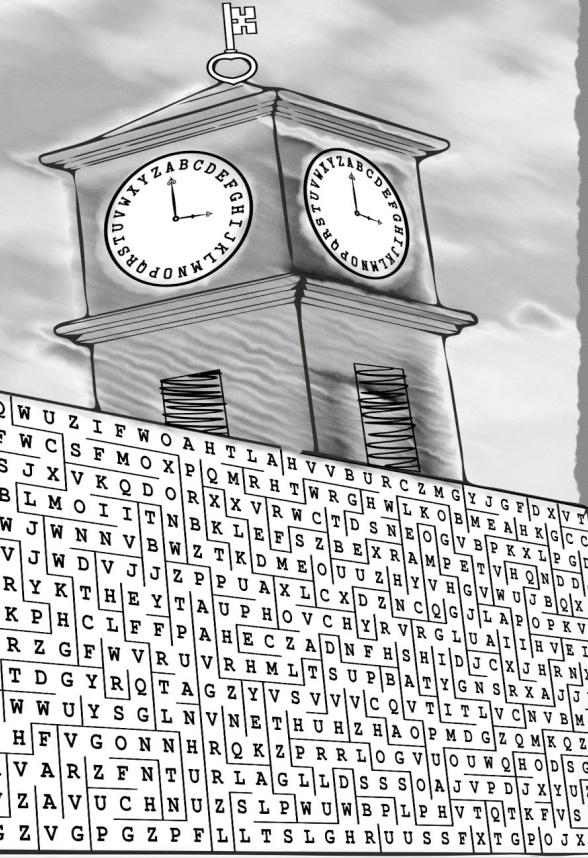


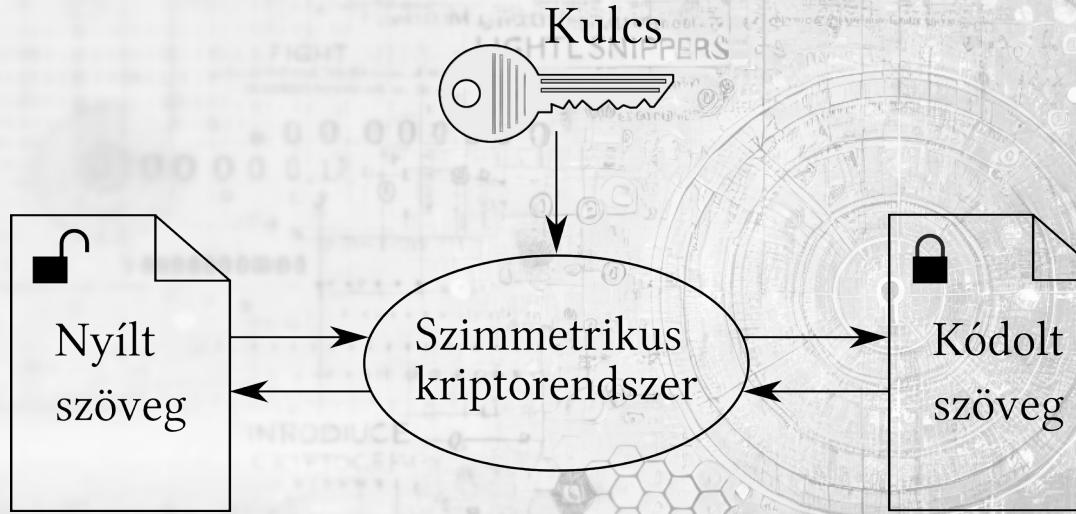
2

Szimmetrikus kulcsú rendszerek

Klasszikus rendszerek

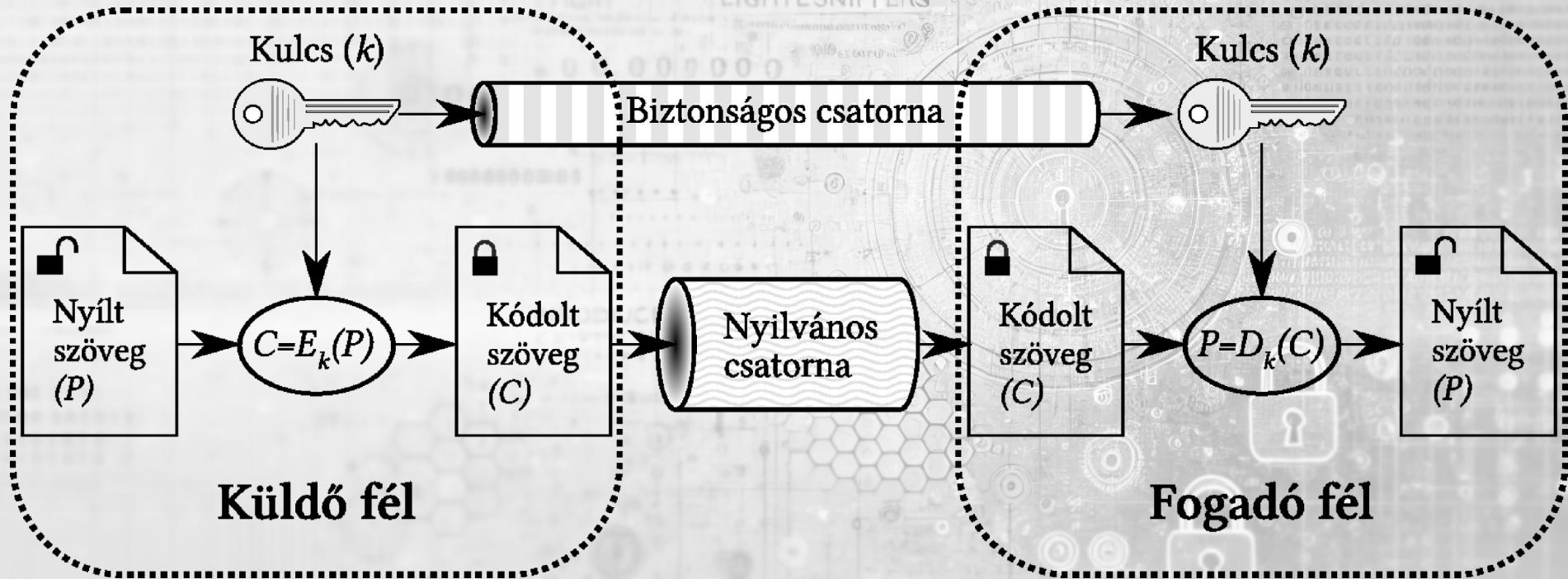


Szimmetrikus kulcsú titkosítás



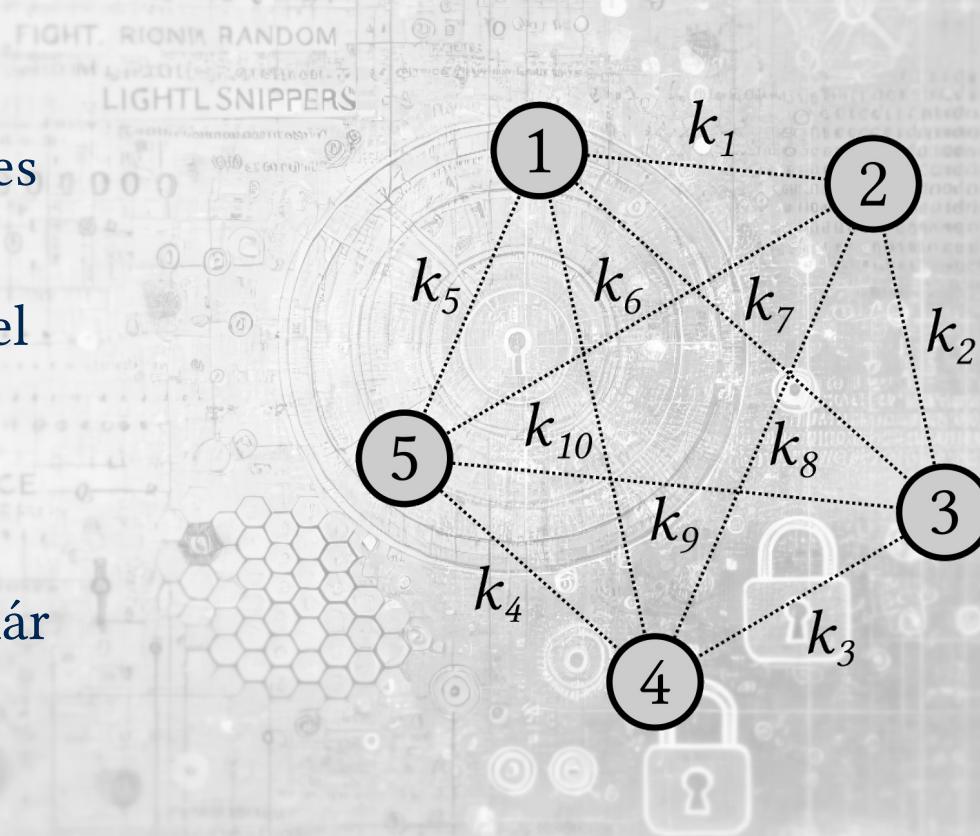
- $C = E_k(P)$
- $P = D_k(C) = E_k^{-1}(E_k(P))$

A kulcscsere problémája



A kulcscsere problémája

- A kulcscserére használt csatorna sokszor költséges és/vagy kockázatos.
- Ha mindenki mindenivel kommunikál, akkor n egyén esetén $n(n-1)/2$ kulcsot kell cserélni.
- Például $n=5$ esetén is már 10 kulcscsere szükséges.



Szimmetrikus kulcsú rendszerek

1. Klasszikus titkosítási rendszerek

- minden olyan egyszerű rejtjelező módszer, amit a történelem folyamán használtak, a legrégebbi időktől a XX. század második feléig
- manapság kevés gyakorlati hasznuk van, inkább didaktikai szempontból érdekesek (a második világháborús rejtjelező gépek kivételével általában „kézi” használatra terveztek őket)
- példák: Caesar-kód, Playfair-kód, Vigenère-rejtjel, átrendezéses kódok, rejtjelező gépek (C-36, Enigma), stb.

Szimmetrikus kulcsú rendszerek

2. Modern titkosítási rendszerek

- gyakorlatban használt módszerek
- használatukhoz számítógép szükséges
- általában titkosított hálózati kommunikációs protokollok részeként működnek
- példák: DES, 3DES, AES, Blowfish, véletlen átkulcsolás (one-time pad), stb.

Klasszikus rendszerek fajtái

1. **Helyettesítő kódok** – Az eredeti szövegegységeket (az ábécé betűi vagy betűcsoportok) egy szabályos rendszer alapján alakítják át rejtjelezett szövegegységekké. A lényeg az, hogy egyazon szövegegységnek minden ugyanaz a kódolt egység felel meg, függetlenül attól, hogy például hol helyezkedik el a szövegen. Ha a szövegegység egy karakter hosszú, akkor a rendszer *monoalfabetikus*, ellenkező esetben *polialfabetikus*.
2. **Átrendezéses (keveréses) kódok** – Az eredeti szöveg egységeit összekeverik (nem ritkán igen bonyolult módszerrel), de maguk a szövegegységek érintetlenül maradnak, vagyis a kódolt szöveg az eredeti szövegnek egy permutációja lesz.
3. **Helyettesítő-átrendező (hibrid) kódok** – Az előző két módszer ötvözete.

A Caesar-kód

Legyen egy n -betűs ábécé, ahol a betűket \mathbb{Z}_n -beli elemekkel azonosítjuk.

Kulcs: $k \in \mathbb{Z}_n$.

Kódolás: $C = E_k(P) = (P + k) \text{ mod } n$, ahol $P \in \mathbb{Z}_n$ (egy betű).

Dekódolás: $P = D_k(C) = (C - k) \text{ mod } n$, ahol $C \in \mathbb{Z}_n$ (egy betű).

A Caesar-kód

- Példa (angol ábécé, $n = 26$):

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Legyen $k = 13$. Ekkor:

$$E_k(\mathbf{T}) = E_k(19) = (19 + 13) \bmod 26 = 6 = \mathbf{G}$$

$$E_k(\mathbf{I}) = E_k(8) = (8 + 13) \bmod 26 = 21 = \mathbf{V}$$

$$E_k(\mathbf{T}) = E_k(19) = (19 + 13) \bmod 26 = 6 = \mathbf{G}$$

$$E_k(\mathbf{O}) = E_k(14) = (14 + 13) \bmod 26 = 1 = \mathbf{B}$$

$$E_k(\mathbf{K}) = E_k(10) = (10 + 13) \bmod 26 = 23 = \mathbf{X}$$

Tehát a **TITOK** szó titkosítva **GVGBX** lesz.

A Caesar-kód

- Caesar-kerék (a kulcs $k=3$):



A Caesar-kód

- Kriptoanalízis:
 - kimerítő kulcskeresés
 - betűgyakoriság-vizsgálat

Gyakoriság	Magyar	Angol
1.	E	E
2.	A	T
3.	T	A
4.	O	O
5.	L/N	I/N



Kulcsszavas Caesar-kód

- A Caesar-kódnak egy változata, segítségével bármilyen megfeleltetést elő lehet állítani (nem csak ciklikus eltolásokat).
 - **Kulcs:** egy (ℓ, s) pár, ahol $\ell \in \mathbb{Z}_n$ és s egy szó (a kulcsszó)
 - **Kódolás:** a megfeleltetési táblázat alsó sorába az ℓ -edik sorszámtól kezdődően beírjuk az s szót (az esetleges ismétlődő betűket kihagyva), majd az ábécé többi betűjét a kulcsszó után írjuk sorrendben, ciklikusan. A kódolás a kapott (betű)permutáció alapján történik.
 - **Dekódolás:** A (betű)permutáció inverze alapján.

Kulcsszavas Caesar-kód

- Példa: $n = 26$ (angol ábécé), $\ell = 8$, $s = \text{CAESAR}$

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
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
Q	T	U	V	W	X	Y	Z	C A E S R	B	D	F	G	H	I	J	K	L	M	N	O	P				

Tehát a **TITOK** szó rejtjelezett formája **JCJDE** lesz.

Kulcsszavas Caesar-kód

- Kriptoanalízis:
 - kimerítő kulcskeresés (rövidebb kulcsszavak esetén)
 - legkisebb négyzetösszeg módszer
 - betűgyakoriság-vizsgálat
 - betűtávolságok mérése

A legkisebb négyzetösszeg módszere

- Legyen A az ábécé betűinek halmaza, $f(a)$ az $a \in A$ betű (százalékos) gyakorisága az adott nyelvben, $f_{D_k(C)}(a)$ az a betű gyakorisága a k kulccsal dekódolt szövegben.
- A jó kulcs k , ha $\sum_{a \in A} (f(a) - f_{D_k(C)}(a))^2$ minimális.
- minden helyettesítő kód esetén működik, de csak akkor használható a módszer, ha a C kódolt szöveg elég hosszú és ha az eredeti P sima szöveg értelmes.

Affin rejtjel

Legyen egy n -betűs ábécé, ahol a betűket \mathbb{Z}_n -beli elemekkel azonosítjuk.

Kulcs: $k = (a, b) \in \mathbb{Z}_n^2$ úgy, hogy létezik $a^{-1} \pmod n$, vagyis $\text{lko}(a, n) = 1$.

Kódolás: $C = E_k(P) = (aP + b) \pmod n$, ahol $P \in \mathbb{Z}_n$ (egy betű).

Dekódolás: $P = D_k(C) = (a^{-1}C - a^{-1}b) \pmod n$, ahol $C \in \mathbb{Z}_n$ (egy betű).

Affin rejtjel

- Példa: $n = 26$ (angol ábécé), $k = (5, 2)$

$$E_k(\mathbf{T}) = E_k(19) = (5 \cdot 19 + 2) \bmod 26 = 19 = \mathbf{T}$$

$$E_k(\mathbf{I}) = E_k(8) = (5 \cdot 8 + 2) \bmod 26 = 16 = \mathbf{Q}$$

$$E_k(\mathbf{T}) = E_k(19) = (5 \cdot 19 + 2) \bmod 26 = 19 = \mathbf{T}$$

$$E_k(\mathbf{O}) = E_k(14) = (5 \cdot 14 + 2) \bmod 26 = 20 = \mathbf{U}$$

$$E_k(\mathbf{K}) = E_k(10) = (5 \cdot 10 + 2) \bmod 26 = 0 = \mathbf{A}$$

Tehát a **TITOK** szó titkosítva **TQTUA** lesz.

Affin rejtjel

- Kriptoanalízis:

- kimerítő kulcskeresés (összesen $n\varphi(n)$ kulcs lehetséges, ahol az Euler-féle számelméleti függvény értéke $\varphi(n) = |\{a \mid 0 \leq a < n, \text{lnko}(a, n) = 1\}|$)
- betűgyakoriság-vizsgálattal elegendő két betű kódolt megfelelőjét megtalálni – legyenek ezek (P_1, C_1) és (P_2, C_2) – ezek segítségével kiszámolható a k kulcs a következő kongruencia alapján:

$$\begin{cases} C_1 = (aP_1 + b) \bmod n \\ C_2 = (aP_2 + b) \bmod n \end{cases} \implies a(P_1 - P_2) \equiv (C_1 - C_2) \pmod{n}$$

Affin rejtjel

Legyen $\lnko(P_1 - P_2, n) = d$.

1. Ha $d = 1$, akkor $a \equiv (P_1 - P_2)^{-1}(C_1 - C_2) \pmod{n}$.
2. Ha $d > 1$, akkor és csakis akkor van megoldás, ha $d \mid (C_1 - C_2)$. Ebben az esetben

$$a \equiv \left(\frac{P_1 - P_2}{d} \right)^{-1} \left(\frac{C_1 - C_2}{d} \right) \pmod{\frac{n}{d}},$$

tehát $a \equiv \left(\frac{P_1 - P_2}{d} \right)^{-1} \left(\frac{C_1 - C_2}{d} \right) + m \frac{n}{d} \pmod{n}$, ahol $m \in \{0, 1, \dots, d-1\}$.

Megj.: Ha $\lnko(a, n) = 1$, akkor $a^{-1} \pmod{n}$ értéke a bővített euklideszi algoritmussal számolható.

Mátrixos affin rejtjel

Legyen egy n -betűs ábécé, ahol a betűket \mathbb{Z}_n -beli elemekkel azonosítjuk, a szöveget $m \geq 2$ hosszúságú tömbökre bontjuk, így a titkosítandó szövegegység:

$$P = \begin{pmatrix} p_1 \\ p_2 \\ \vdots \\ p_m \end{pmatrix} \in \mathbb{Z}_n^m.$$

Mátrixos affin rejtjel

Kulcs: $k = (A, b)$, ahol $A = (a_{ij}) \in \mathcal{M}_m(\mathbb{Z}_n)$ egy $m \times m$ -es invertálható mátrix \mathbb{Z}_n felett (vagyis $\lnko(\det A, n) = 1$) és

$$b = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix} \in \mathbb{Z}_n^m.$$

Kódolás: $C = E_k(P) = AP + b$, vagyis

$$\begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_m \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1m} \\ a_{21} & a_{22} & \cdots & a_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mm} \end{pmatrix} \begin{pmatrix} p_1 \\ p_2 \\ \vdots \\ p_m \end{pmatrix} + \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix}.$$

Dekódolás: $P = A^{-1}(C - b)$.

Mátrixos affin rejtjel

- Kriptoanalízis:
 - Csak kódolt üzenet ismeretén alapuló támadás
 - kimerítő kulcskeresés (kb. $\varphi(n)n^{m^2+m-1}$ lehetséges kulcs)
 - szövegegységek gyakoriságának vizsgálata (ha m elég kicsi)
 - Nyílt szöveg ismeretén alapuló támadás
 - ismerni kell $m+1$ darab eredeti üzenetet, kódolt megfelelőikkal együtt ahhoz, hogy lineáris kongruencia-rendszerből megkapjuk a $k = (A, b)$ kulcsot

Mátrixos affin rejtjel

Tegyük fel, hogy ismerünk $m+1$ darab (P^i, C^i) párt.

Ha $P^i = \begin{pmatrix} p_1^i \\ \vdots \\ p_m^i \end{pmatrix}$ és $C^i = \begin{pmatrix} c_1^i \\ \vdots \\ c_m^i \end{pmatrix}$, akkor a rendszer (mátrix alakban):

$$\begin{pmatrix} c_1^1 - b_1 & \dots & c_1^{m+1} - b_1 \\ \vdots & \ddots & \vdots \\ c_m^1 - b_m & \dots & c_m^{m+1} - b_m \end{pmatrix} = \begin{pmatrix} a_{11} & \dots & a_{1m} \\ \vdots & \ddots & \vdots \\ a_{m1} & \dots & a_{mm} \end{pmatrix} \begin{pmatrix} p_1^1 & \dots & p_1^{m+1} \\ \vdots & \ddots & \vdots \\ p_m^1 & \dots & p_m^{m+1} \end{pmatrix},$$

ahol az $m^2 + m = m(m+1)$ darab ismeretlen (a_{ij}) és b_j , $i, j = \overline{1, m}$. Látható, hogy

van $m(m + 1)$ darab egyenlet. Ha $b = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$, akkor elegendő m darab (P^i, C^i) pár.

Vigenère-rejtjel

A Vigenère-tábla („tabula recta”) egy 26×26 -os tábla, melynek első sora az ábécé betűiből áll, ábécé sorrendben, a második sora az első sor ciklikusan balra tolva egy betűvel, a harmadik sora a második sor ciklikusan balra tolva egy betűvel és így tovább.

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

Vigenère-rejtjel

Kulcs: A kulcs egy szó, melynek egymásutáni ismétlésével megkapjuk a kulcsszöveget. A kulcs hosszát periódusnak nevezzük.

Kódolás: A kódolt szöveg k -adik betűjét a következő módon kapjuk meg: megkeressük az eredeti szöveg k -adik betűjét (mondjuk ez az ábécé i -edik betűje) és a kulcsszöveg k -adik betűjét (mondjuk ez az ábécé j -edik betűje); ekkor a kódolt betű a Vigenère-tábla i -edik sorában és j -edik oszlopában levő betű (a tábla szimmetrikus).

Dekódolás: Az eredeti szöveg k -adik betűjét a következő módon kapjuk vissza: ha a kulcsszöveg k -adik betűje az i -edik az ábécében, akkor a tábla i -edik sorában megkeressük a kódolt szöveg k -adik betűjét. Tételezzük fel, hogy ez az i -edik sor j -edik pozíciójában van. Ekkor az eredeti betű az ábécé j -edik betűje.

Vigenère-rejtjel

A Vigenère-rejtjel egy partikuláris mátrixos affin rendszer, ahol $n = 26$, $A = I_m$ és b az m hosszúságú kulcsszó.

Akkor m betűs tömböként kódolva igaz, hogy $C = E_k(P) = I_m P + b = P + b$, vagyis:

$$\begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_m \end{pmatrix} = \begin{pmatrix} p_1 \\ p_2 \\ \vdots \\ p_m \end{pmatrix} + \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix} \text{ mod } 26,$$

ahol $P = \begin{pmatrix} p_1 \\ p_2 \\ \vdots \\ p_m \end{pmatrix}$ a nyílt szöveg és $C = \begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_m \end{pmatrix}$ a kódolt üzenet.

Vigenère-rejtjel

- Példa: Az eredeti szöveg legyen GIVETHEMUP, a kulcs pedig TEA. Ekkor a kulcsszöveg TEATEATEAT (ugyanolyan hosszú, mint az eredeti szöveg). A kódolt szöveg ZMVXXHXQUI lesz. Mátrixos affin rendszerként nézve így lehet számolni:

$$\begin{pmatrix} \mathbf{G} \\ \mathbf{I} \\ \mathbf{V} \end{pmatrix} + \begin{pmatrix} \mathbf{T} \\ \mathbf{E} \\ \mathbf{A} \end{pmatrix} = \begin{pmatrix} 6 \\ 8 \\ 21 \end{pmatrix} + \begin{pmatrix} 19 \\ 4 \\ 0 \end{pmatrix} = \begin{pmatrix} 25 \\ 12 \\ 21 \end{pmatrix} = \begin{pmatrix} \mathbf{Z} \\ \mathbf{M} \\ \mathbf{V} \end{pmatrix}$$

$$\begin{pmatrix} \mathbf{E} \\ \mathbf{T} \\ \mathbf{H} \end{pmatrix} + \begin{pmatrix} \mathbf{T} \\ \mathbf{E} \\ \mathbf{A} \end{pmatrix} = \begin{pmatrix} 4 \\ 19 \\ 7 \end{pmatrix} + \begin{pmatrix} 19 \\ 4 \\ 0 \end{pmatrix} = \begin{pmatrix} 23 \\ 23 \\ 7 \end{pmatrix} = \begin{pmatrix} \mathbf{X} \\ \mathbf{X} \\ \mathbf{H} \end{pmatrix}$$

$$\begin{pmatrix} \mathbf{E} \\ \mathbf{M} \\ \mathbf{U} \end{pmatrix} + \begin{pmatrix} \mathbf{T} \\ \mathbf{E} \\ \mathbf{A} \end{pmatrix} = \begin{pmatrix} 4 \\ 12 \\ 20 \end{pmatrix} + \begin{pmatrix} 19 \\ 4 \\ 0 \end{pmatrix} = \begin{pmatrix} 23 \\ 16 \\ 20 \end{pmatrix} = \begin{pmatrix} \mathbf{X} \\ \mathbf{Q} \\ \mathbf{U} \end{pmatrix}$$

$$\mathbf{P} + \mathbf{T} = 15 + 19 = 8 = \mathbf{I}$$

Vigenère-rejtjel

- Kriptoanalízis:
 - ha tudjuk az m periódust, akkor m darab Caesar-kódöt kell feltörni
 - ha nem ismert az m , akkor a Kasiski-módszerrel lehet próbálkozni (az ismétlődő betűsorozatok megkeresése a titkosított szövegben, és a sorozatok közötti távolságok felhasználása a kulcs hosszának meghatározásához)

Playfair-kód

Kulcs: A kulcs egy 5×5 -ös betűtábla, melyben az angol ábécé betűi szerepelnek a J kivételével. Ezt a betűtáblát egy kulcsszó segítségével is ki lehet tölteni a kulcsszavas Caesar-kódnál megismert módon: a kulcsszó (betűismétlések nélkül) a legfelső sor bal sarkából indul balról jobbra és fentről lefele (ha 5 betűnél hosszabb); a kimaradt betűk ábécésorrendben követik a kulcsszót balról jobbra és fentről lefele.

Kódolás: A kódolás betűpáronként történik, ehhez a szöveget betűpárokra bontjuk, az esetleges J betűket I-re cserélve. Ha egy betűpárban kétszer szerepel ugyanaz a betű, akkor az első betű után egy X-et szúrunk be. Ha a betűk száma páratlan, akkor a szöveget egy X-szel egészítjük ki a végén. A betűpárokat három eset szerint a következő módon kódoljuk:

Playfair-kód

1. Ha a betűpár betűi a tábla azonos sorában vannak, akkor a táblában ciklikusan jobbra toljuk őket egy pozícióval.
2. Ha a betűpár betűi a tábla azonos oszlopában vannak, akkor ciklikusan lefelé toljuk őket egy pozícióval.
3. Ha a betűpár betűi nincsenek sem azonos sorban, sem azonos oszlopban, akkor a táblában az általuk (áttellenes csúcsokként) meghatározott téglalap másik két átellenes csúcsába kódolódnak úgy, hogy az eredeti betűpár első betűje és a kódolt betűpár első betűje egy sorban legyenek.

Dekódolás: Ugyanúgy történik, mint a kódolás, csak az első esetben ciklikusan balra tolunk egy pozícióval és a második esetben ciklikusan felülről tolunk egy pozícióval.

Playfair-kód

- Példa: Ha a kulcsszó MOON, akkor a következő Playfair-tábla alapján a a JIMMYS szót így titkosítjuk:

JIMMYS → IIMMYS → IX IM MY SX → KWHOAVXN

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

Playfair-kód

- Kriptoanalízis:

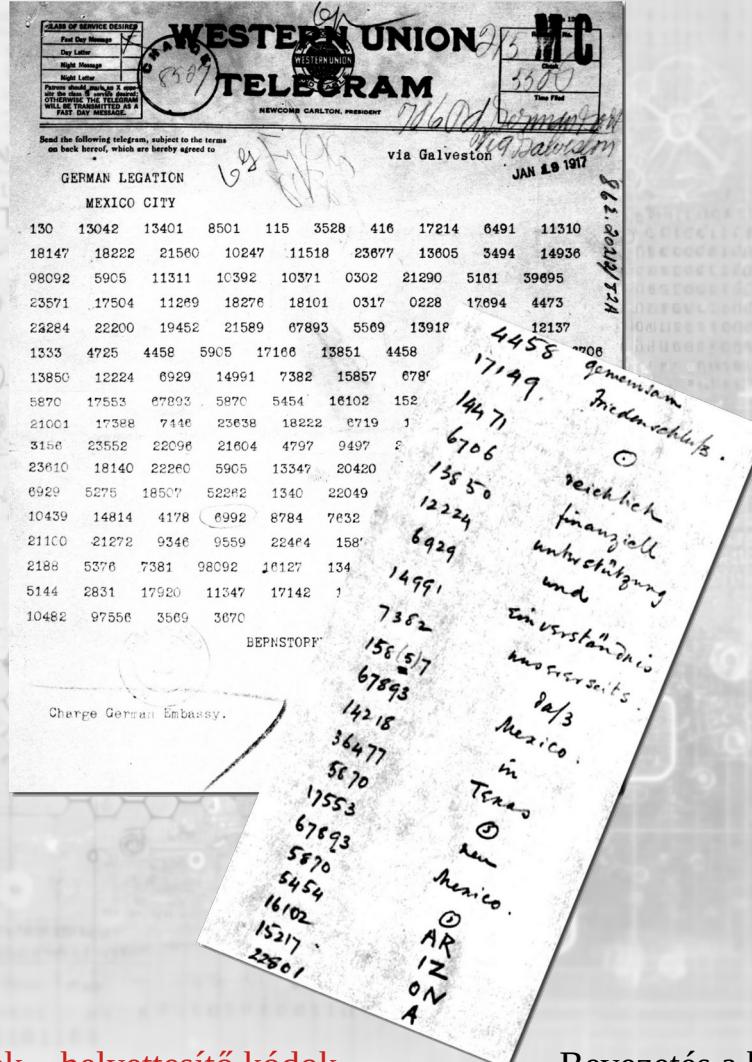
- a kimerítő kulcskeresés gyakorlatban nem kivitelezhető ($25! = 15511210043330985984000000$ lehetséges tábla)
- a betűpárgyakoriság-vizsgálat csökkentheti a lehetséges kulcsok számát
- ha a kulcsszó rövid, betűtávolság-mérés

Kódkönyv

- A kódkönyv egy kétirányú szótár, számcsoportokat, esetleg (értelmetlen vagy értelmes) szavakat feleltet meg betűcsoportoknak, szavaknak, szócsoportoknak vagy akár rövid mondatoknak.
- Mindkét félnek (küldő és vevő) rendelkeznie kell a kódkönyvvel ahoz, hogy kommunikálni tudjanak.
- Fő előnye a nehéz feltörhetőség.
- Fő hátránya a kódkönyvek biztonságának garantálása.

Kódkönyv

- Példa: a Zimmermann-távirat (első világháború)



Cikkcakk rejtjel

Kulcs: $k \in \mathbb{N}$, $k \geq 2$

Kódolás: A nyílt szöveg betűit egy szakaszonként k betűből álló cikcakkos tört vonal mentén leírjuk, majd a vízszintes sorok mentén olvasott betűket egymás mellé írjuk.

Cikkcakk rejtjel

Dekódolás: A dekódolást legkönnyebb egy négyzetes lapon vagy egy táblázat segítségével végezni. Mivel tudjuk a k kulcsot, azt is tudjuk, hogy milyen alakja lesz cikcakkos vonalnak (és a kódolt szöveg hossza alapján azt is, hogy a vonal milyen hosszú lesz). Megjelöljük azokat a négyzeteket, ahova betű fog kerülni, majd vízszintes soronként haladva kitöltjük a megjelölt négyzeteket a kódolt szöveg egymás utáni betűivel. Így visszakapjuk a kódolásnál használt cikcakkos betűtáblázatot, és olvashatóvá válik a nyílt üzenet.

Cikkcakk rejtel

- Példa: Ha $k = 4$ és $P = \text{„Tape at war you one a wash on.”}$, akkor $C = \text{„TWOSATAUNAHPAROEWOEYAN”}$

- Kriptoanalízis: kimerítő kulcskeresés

Útvonal kód

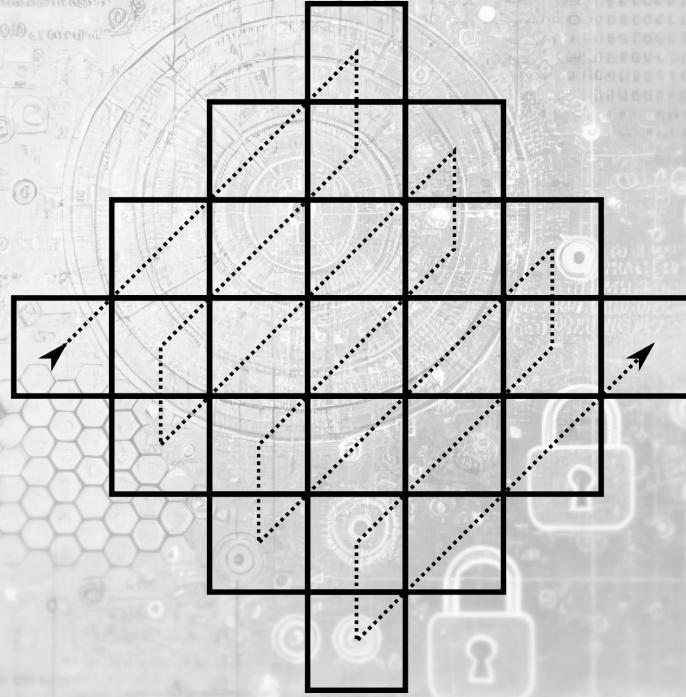
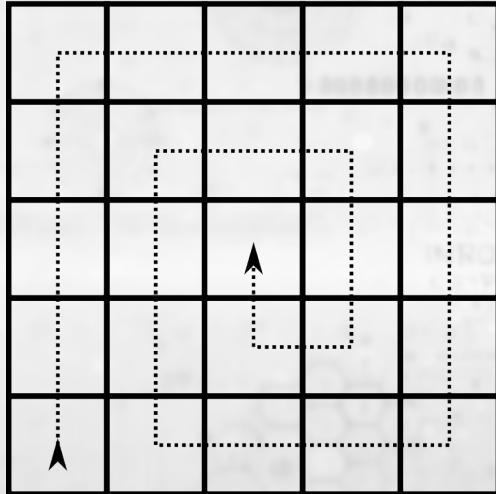
Kulcs: A kulcs gyakorlatilag magának a titkosítási módszernek az ismerete: a fogadó félnek tudnia kell a rács alakját, azt hogy milyen sorrendben volt beírva az eredeti szöveg, és milyen „útvonalon” kell kiolvasni azt a rácsból.

Kódolás: A küldő fél beírja a rácsba az eredeti üzenet betűit a kulcsban foglalt utasításoknak megfelelően.

Dekódolás: A titkos üzenet címzettje felépíti ugyanazt a rácsos betűstruktúrát amit a kódoló is használt, majd kiolvassa a rácsból az üzenetet.

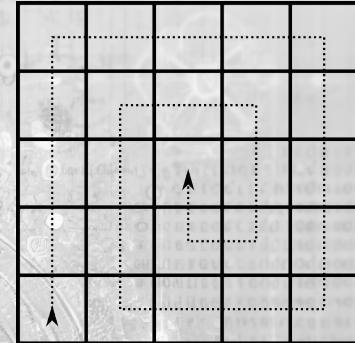
Útvonal kód

Két lehetséges kulcs:



Útvonal kód

- Példa:
 - $k = „5 \times 5$ -ös négyzetrács, a nyílt szöveg soronként lefele és soron belül balról jobbra volt beírva, a kódolt szöveget a következő útvonalon olvasd ki: spirálisan befele haladva a rács bal alsó sarkától indulva felfele.”
 - $P = „If you one door how I mace, I'm egg!”$
 - $C = „IIOOI FYOUO WEGGE MMRNE DOCAH”$



A 5x5 grid of letters in a bold, black serif font. The letters are arranged as follows:
Row 1: I, F, Y, O, U
Row 2: O, N, E, D, O
Row 3: O, R, H, O, W
Row 4: I, M, A, C, E
Row 5: I, M, E, G, G
The background of the grid features a faint, repeating pattern of mechanical or gear-like shapes.

Oszlopos transzpozíció

Kulcs: Egy különböző betűkből álló, maximálisan n hosszúságú szó, ahol n a használt ábécé betűinek száma (ha kulcsnak mégis egy olyan értelmes szót választunk, amiben vannak betűismétlések, akkor az ismétlődő betűket kihagyjuk).

Kódolás: A rács téglalap alakú, a kulcs hossza határozza meg az oszlopok számát, az üzenet hossza pedig a sorokét (a kulcs hossza egyenlő az oszlopok számával). A rácsba beírjuk a sima szöveget (soronként, balról jobbra). Ezután a kulcsszót a rács fölé írjuk úgy, hogy minden egyes betűje egy-egy oszlop fölé kerüljön, majd oszloponként kiolvassuk és egymás mellé írjuk a rácsban levő betűket. A kulcsszó betűinek sorszáma fogja meghatározni az oszlopok olvasásának sorrendjét. Ha a téglalap alakú rács nem telik meg teljesen az eredeti üzenet betűivel, akkor az üres négyzeteket X betűkkel tölthetjük ki, de akár üresen is hagyhatjuk őket.

Oszlopos transzpozíció

Dekódolás: A kulcs és a rejtjelezett szöveg ismeretében oszloponként fel lehet építeni a rácsot, amiből az eredeti üzenet kiolvasható.

- Kriptoanalízis: próbálgatással megtalálható a rács sorainak száma, és ha a kódolt szöveg értelmes, akkor anagrammák keresésével innen már nem nehéz (a kulcs ismerete nélkül) kitalálni az oszlopok helyes sorrendjét.

Oszlopos transzpozíció

Példa:

$k = \text{"HONORIFICABILITUDINITAS"}$

$P = \text{"Reginam occidere nolite timere bonum est si omnes consentiunt ego non contradico."}$ *

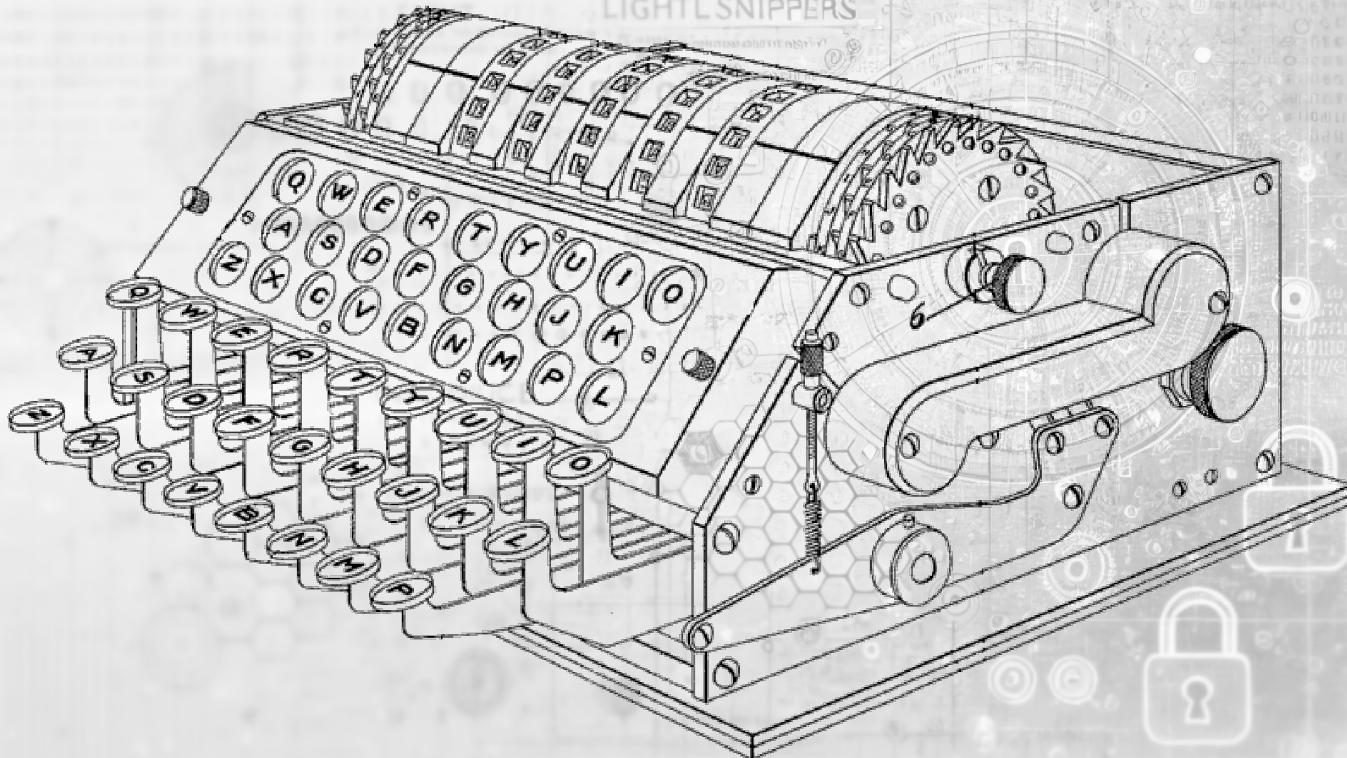
$C = \text{"OTSIR CIIUA METTT EEEGO ATSNN REOCN NIEEO CMOND GOUNN ENNOO ILMSC RBSOX IEMTI DRNEC"}$

* „A királynét megölni nem kell félnetek jó lesz ha mindenki egyetért én nem ellenzem.” (Merániai János esztergomi érsek, 1213)

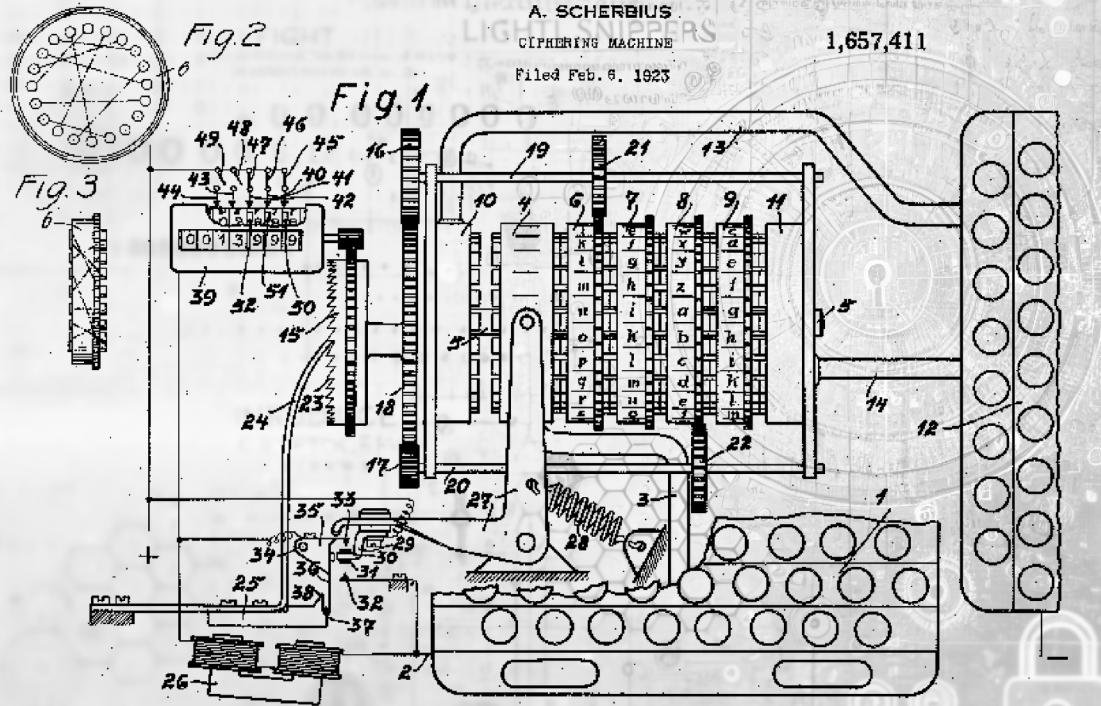
A 5x13 grid for a columnar transposition cipher. The top row contains the key letters H O N R I F C A B L T U D S. The bottom row contains the corresponding letters from the plaintext: R E G I N A M O C C I D E R, E N O L I T E T I M E R E B, O N U M E S T S I O M N E S, C O N S E N T I U N T E G O, and N O N C O N T R A D I C O X.

H	O	N	R	I	F	C	A	B	L	T	U	D	S
R	E	G	I	N	A	M	O	C	C	I	D	E	R
E	N	O	L	I	T	E	T	I	M	E	R	E	B
O	N	U	M	E	S	T	S	I	O	M	N	E	S
C	O	N	S	E	N	T	I	U	N	T	E	G	O
N	O	N	C	O	N	T	R	A	D	I	C	O	X

Rejtjelező gépek

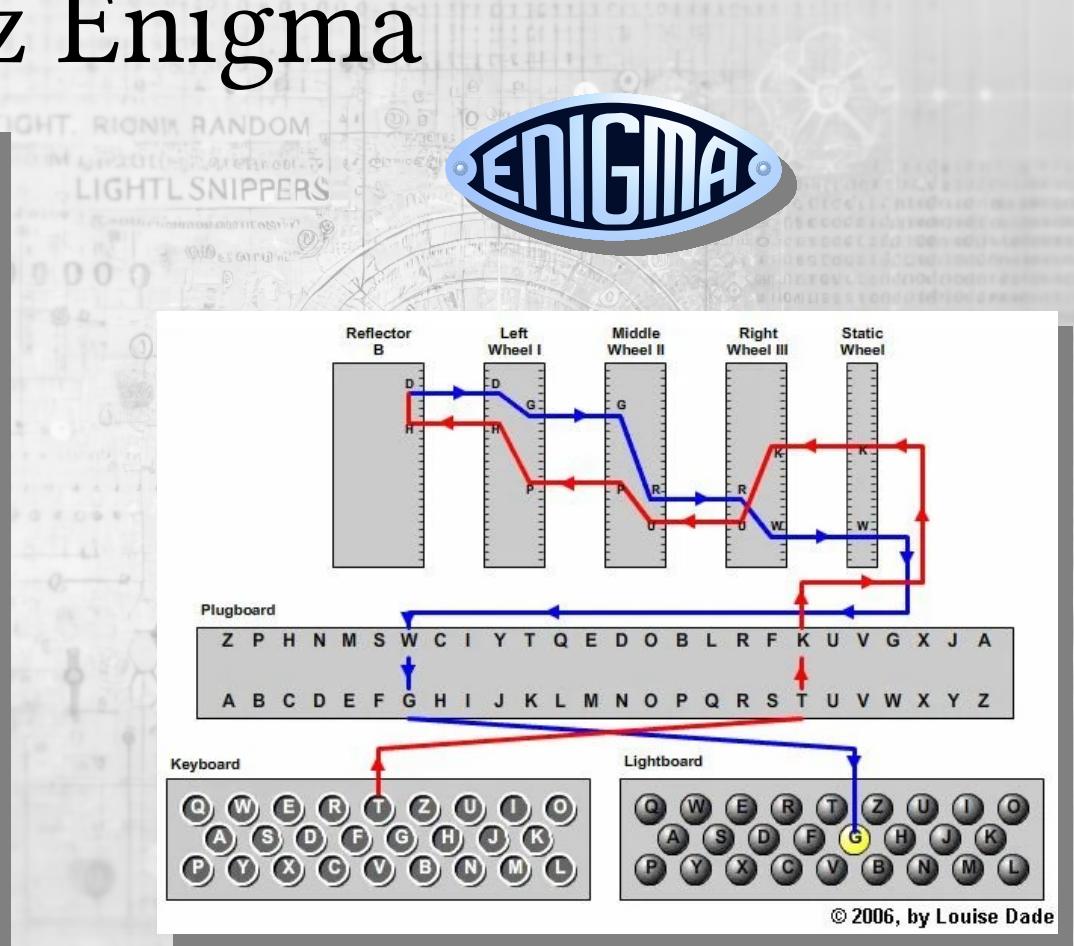


Az Enigma

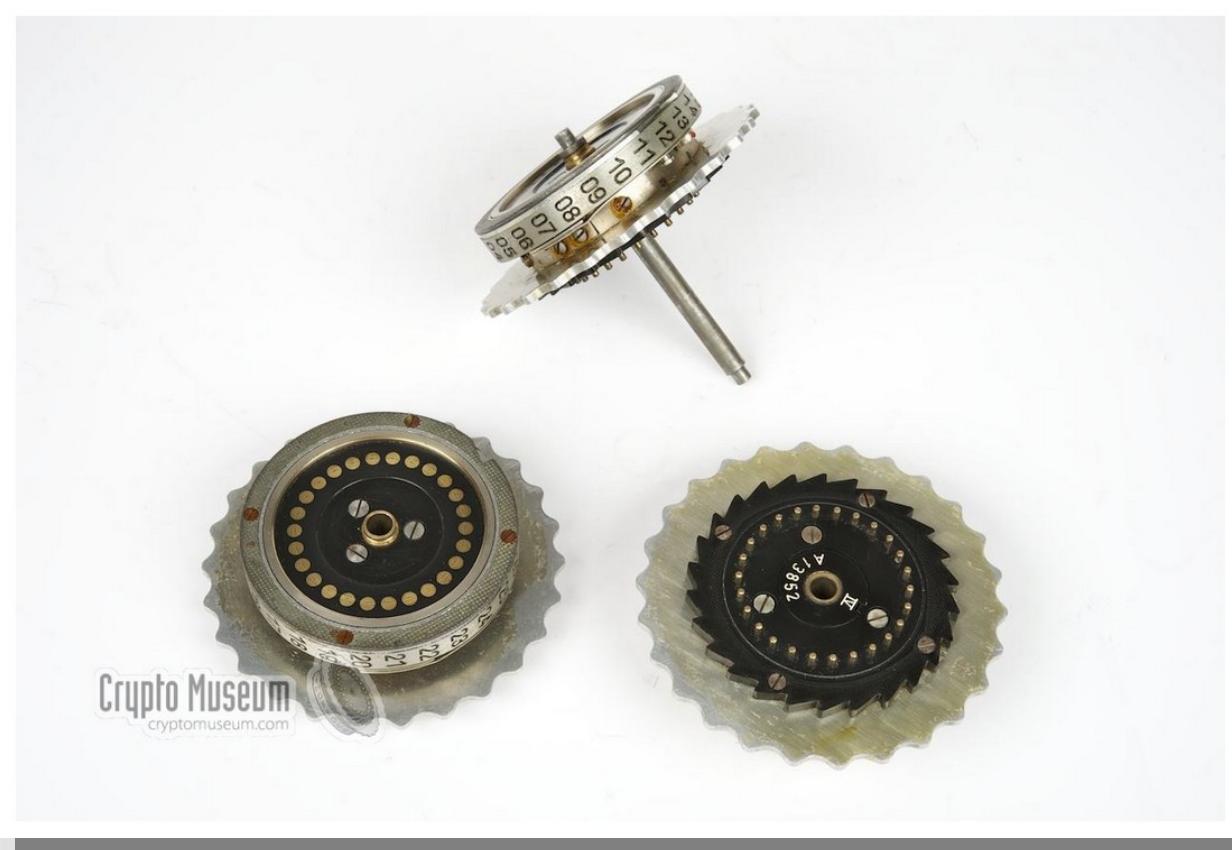


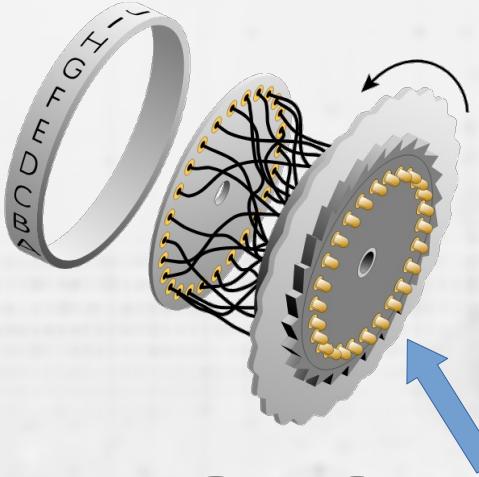
Inventor
A. Scherbius,
By Markublik Atty.

Az Enigma

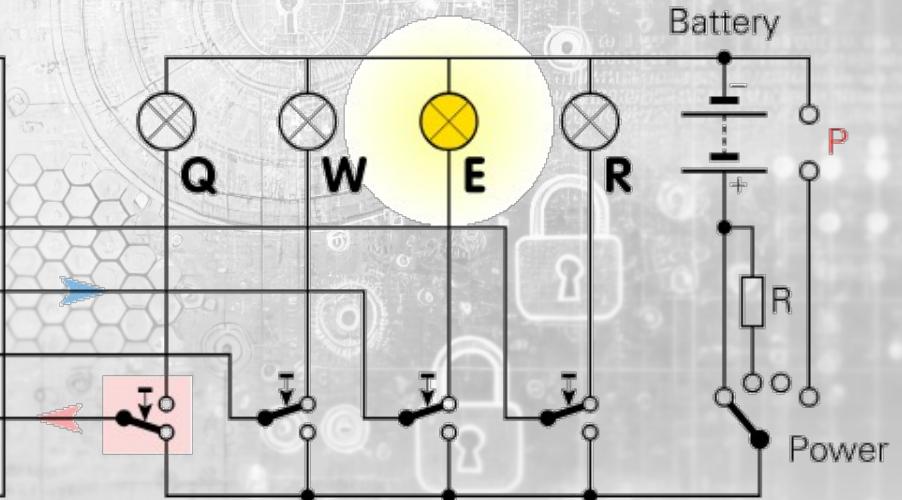
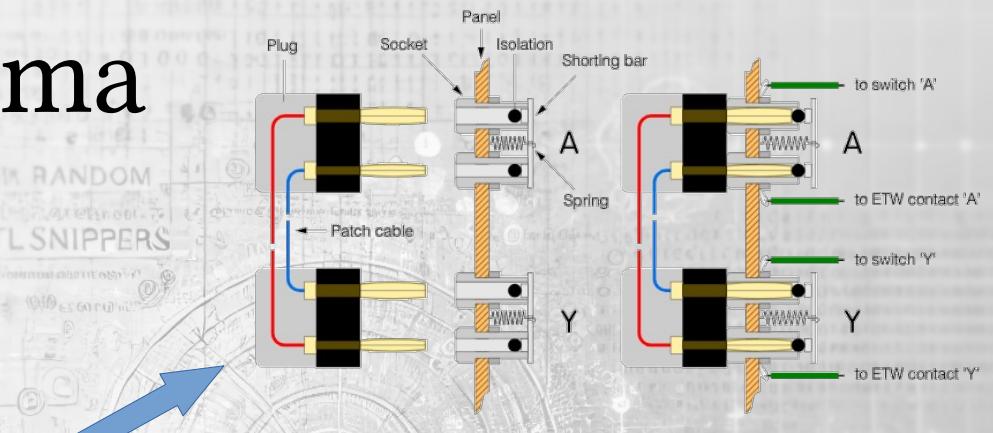
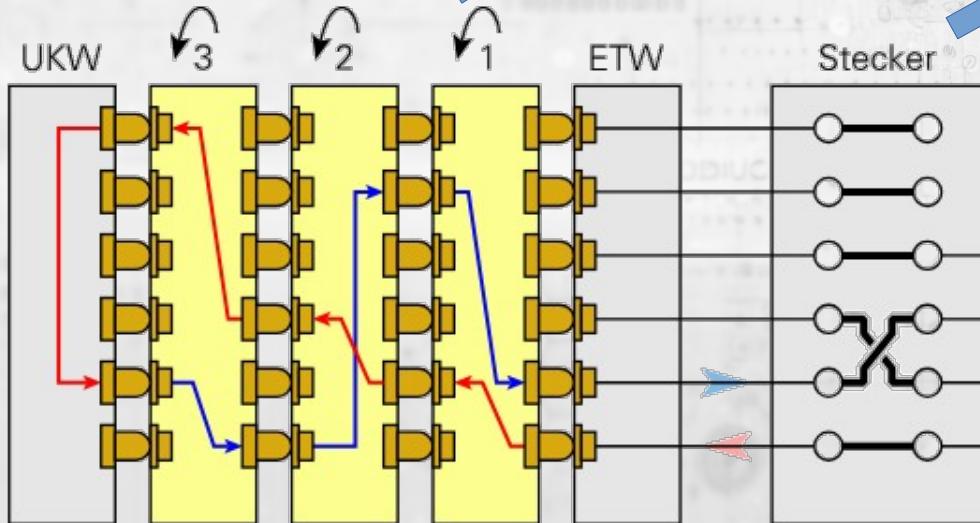


Az Enigma





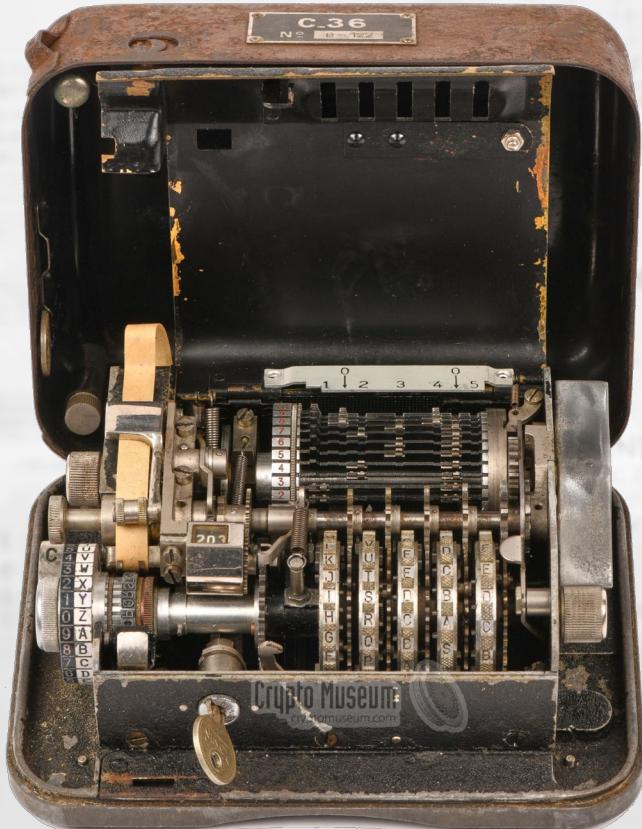
Az Enigma



Az Enigma

- <https://enigma.virtualcolossus.co.uk/>
- <https://www.scienceabc.com/innovation/the-imitation-game-how-did-the-enigma-machine-work.html>
- <https://williame.github.io/post/145830743193.html>
- http://wiki.franklinheath.co.uk/index.php/Enigma_Paper_Enigma

A C-36-os rejtjelező gép



② Szimmetrikus kulcsú rendszerek



Bevezetés a kriptográfiába

A C-36-os rejtjelező gép

A C-36 matematikai modelljének alapja két mátrix:

1. A cipelő mátrix (lug matrix) $M \in \mathcal{M}_{6,27}(\mathbb{Z}_2)$ egy 6×27 -es bináris mátrix azzal a tulajdonsággal, hogy minden oszlopból legtöbb két darab 1-es van.
2. A lépcsőforma (step figure). Ennek első sora 17, második sora 19, harmadik sora 21, negyedik sora 23, ötödik sora 25, hatodik sora pedig 26 dimenziós bináris vektor. Jelöljük ezeket s_1, s_2, \dots, s_6 -tal.

A C-36-os rejtjelező gép

A lépcsőforma segítségével generálni lehet egy 6 soros mátrixot, aminek tetszőleges számú oszlopa van (az előbbi bináris sorvektorok egymás utáni ismétlésével).

Jelölje v_i az N mátrix i -edik oszlopát.

$$N = \begin{pmatrix} s_1 & s_1 & s_1 & \dots \\ s_2 & s_2 & s_2 & \dots \\ \vdots & \vdots & \vdots & \\ s_6 & s_6 & s_6 & \dots \end{pmatrix}.$$

A C-36-os rejtjelező gép

- Példa: lépcsőforma, ahol $v_1 = (010000)$, $v_{17} = (011110)$, $v_{18} = (010000)$, $v_{19} = (100111)$, $v_{20} = (111010)$.

1	2	3	4	5	...	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	...
0	1	1	0	1	...	1	0	0	1	1	0	1	0	1	...							
1	0	0	1	1	...	0	1	1	0	1	0	0	1	1	...							
0	0	1	0	1	...	1	1	0	0	1	0	0	0	1	0	1	...					
0	1	0	0	0	...	0	1	0	1	0	1	0	1	0	1	0	0	0	...			
0	0	1	0	0	...	1	1	0	1	1	1	1	1	1	0	0	0	1	0	0	...	
0	1	0	1	0	...	1	0	0	1	0	0	1	0	0	0	1	0	1	0	...		

A C-36-os rejtjelező gép

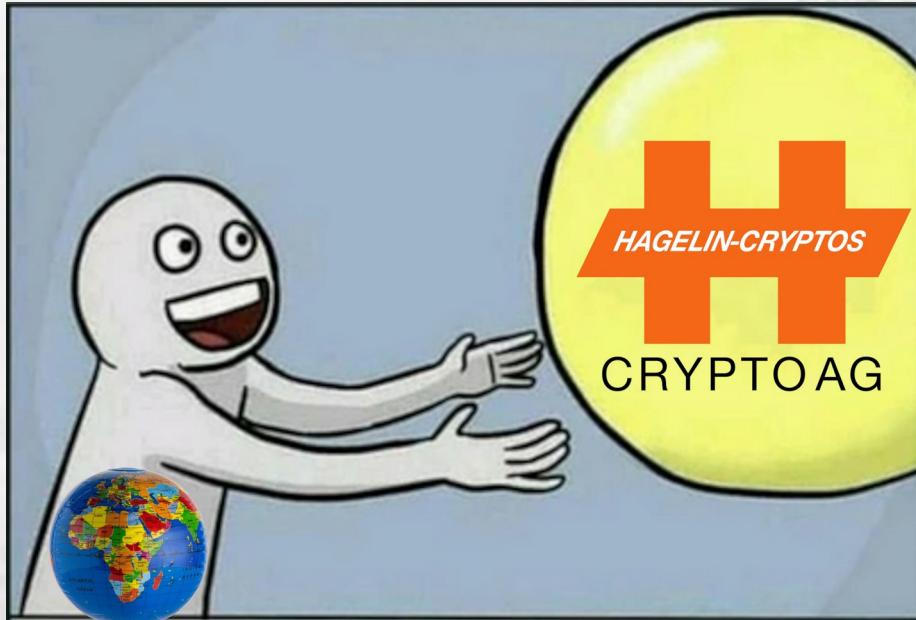
Kulcs: $k = (M, N)$ mátrixpár.

Kódolás: Betűnkét történik. Ha P_i a nyílt szöveg i -edik betűje, akkor $C_i = h_i - P_i - 1$, ahol C_i a kódolt szöveg i -edik betűje, h_i pedig $v_i M$ -ben a nem nulla elemek száma.

Dekódolás: $P_i = h_i - C_i - 1$.

- Kriptoanalízis: A C-36 ekvivalens egy $p = 17 \cdot 19 \cdot 21 \cdot 23 \cdot 25 \cdot 26 = 101405850$ periódusú (ellentétes előjelű) Vigenère-rejtjellel.

Crypto AG



- <https://www.washingtonpost.com/graphics/2020/world/national-security/cia-cryptographic-encryption-machines-espionage/>
- <https://www.crypto.ch/>