

Matematikus kódjátzmák

Kriptográfia Julius Caesartól a kvantumkomputerig

Nagy Gábor Péter

Szegedi Tudományegyetem
Bolyai Intézet

Radnóti Gimnázium Tudományos Hét
2024. október 15.

Tagolás

- 1 A titkosítások elméleti alapelvei
- 2 Az Enigma-rendszerek működése
- 3 Az Enigma sebezhetőségei
- 4 Napjaink kriptorendszerei

Table of Contents

- 1 A titkosítások elméleti alapelvei
- 2 Az Enigma-rendszerek működése
- 3 Az Enigma sebezhetőségei
- 4 Napjaink kriptorendszerei

Titkosírások tudományos alapja

A történeti háttér:

- A titkosírások modern módszerei a **19. század elejétől** terjedtek el.
- Ezeket a mai napig elsősorban **katonai** vagy **üzleti célokra** használják.
- Ekkortól próbálják a titkosítási technikákat **tudományos alapokra** helyezni

A KRIPTOANALÍZIS tudományos módszerei:

- **Hagyományos:** Nyelvészet, matematikai statisztika
- **Modern:** Absztrakt algebra, bonyolultságelmélet, számítástudomány, elliptikus görbék, pseudo-véletlen sorozatok, kvantumalgoritmusok

Titkosírások tudományos alapja

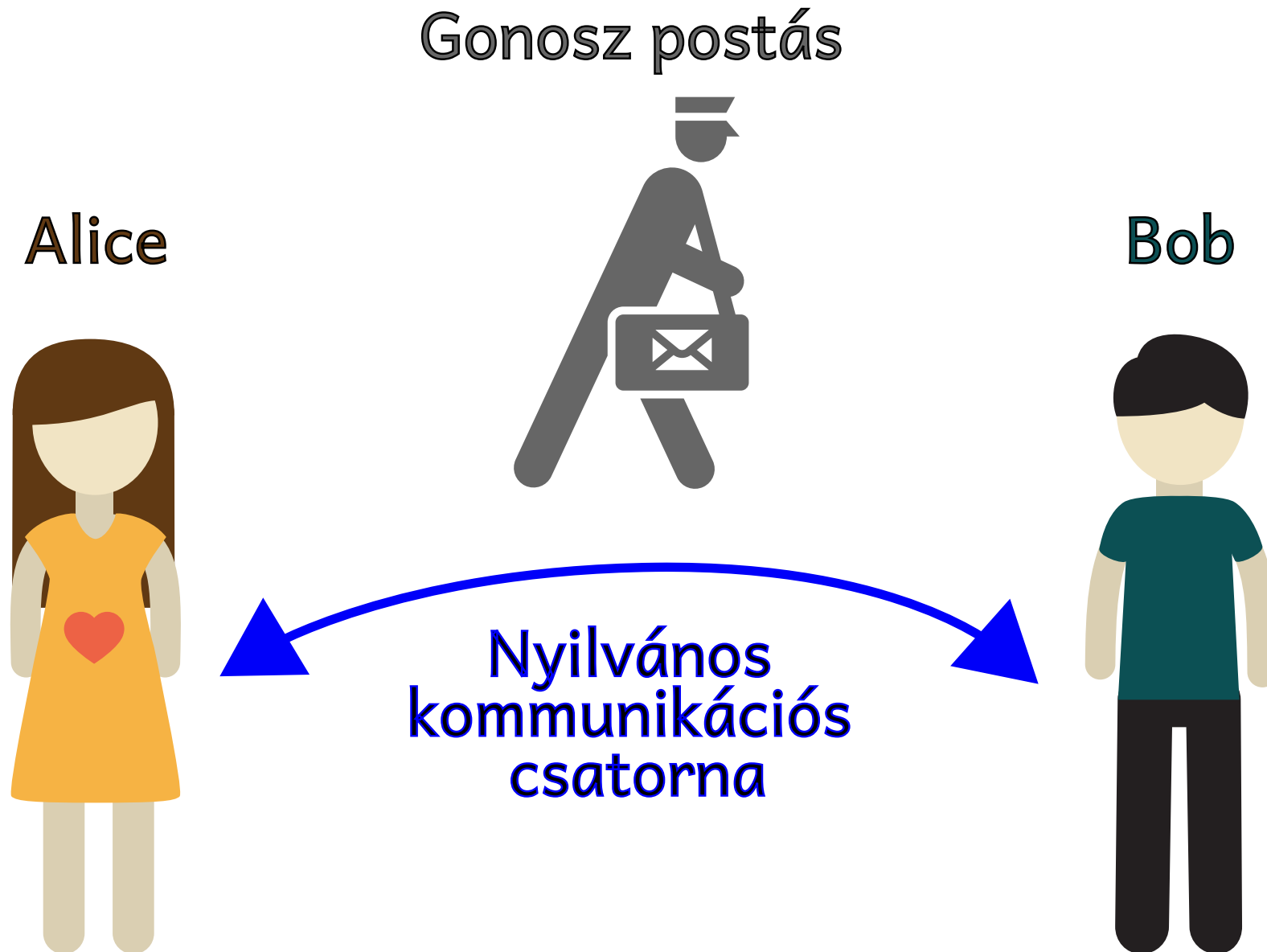
A történeti háttér:

- A titkosírások modern módszerei a **19. század elejétől** terjedtek el.
- Ezeket a mai napig elsősorban **katonai** vagy **üzleti célokra** használják.
- Ekkortól próbálják a titkosítási technikákat **tudományos alapokra** helyezni

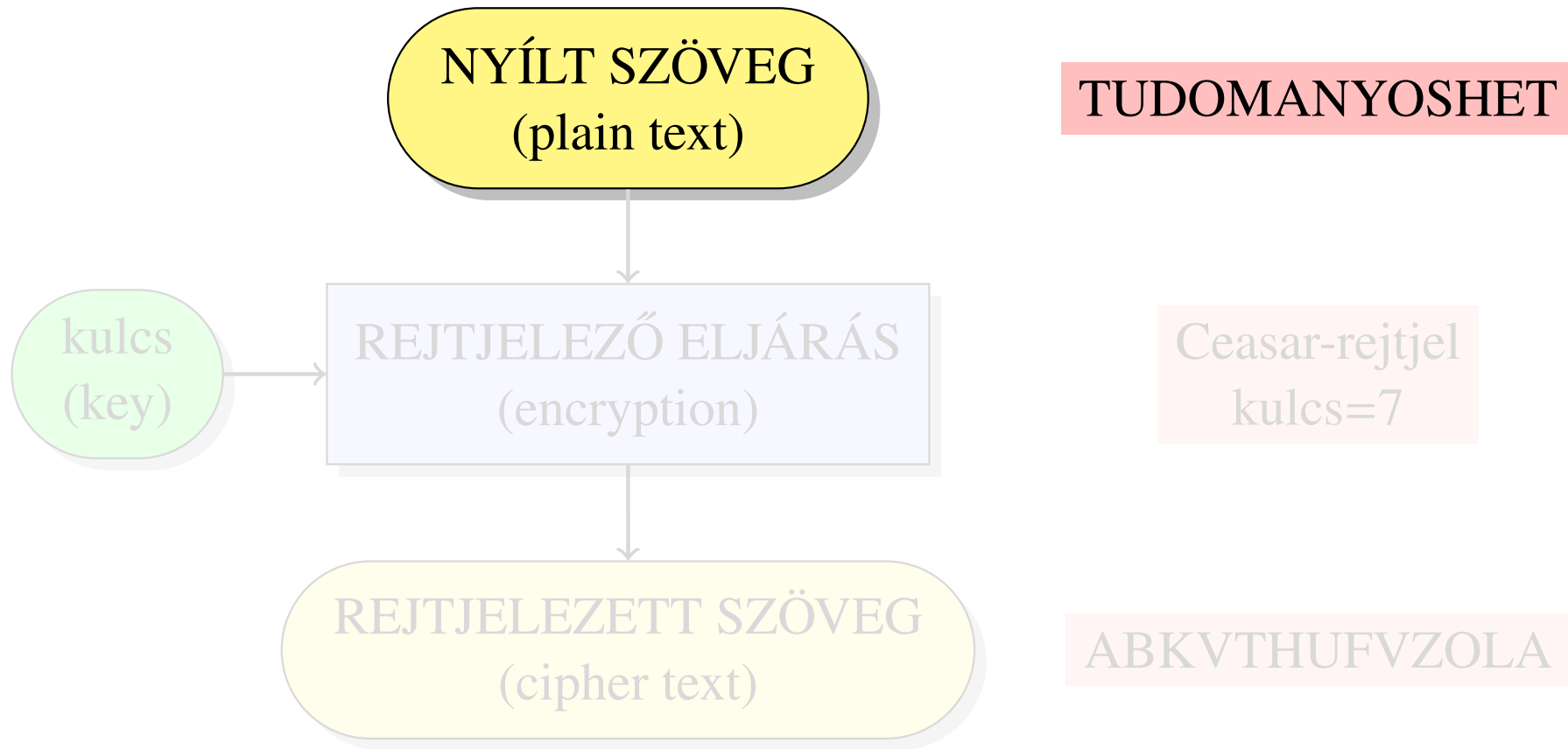
A KRIPTOANALÍZIS tudományos módszerei:

- **Hagyományos:** Nyelvészet, matematikai statisztika
- **Modern:** Absztrakt algebra, bonyolultságelmélet, számítástudomány, elliptikus görbék, pseudo-véletlen sorozatok, kvantumalgoritmusok

A kriptográfia kommunikációs sémája



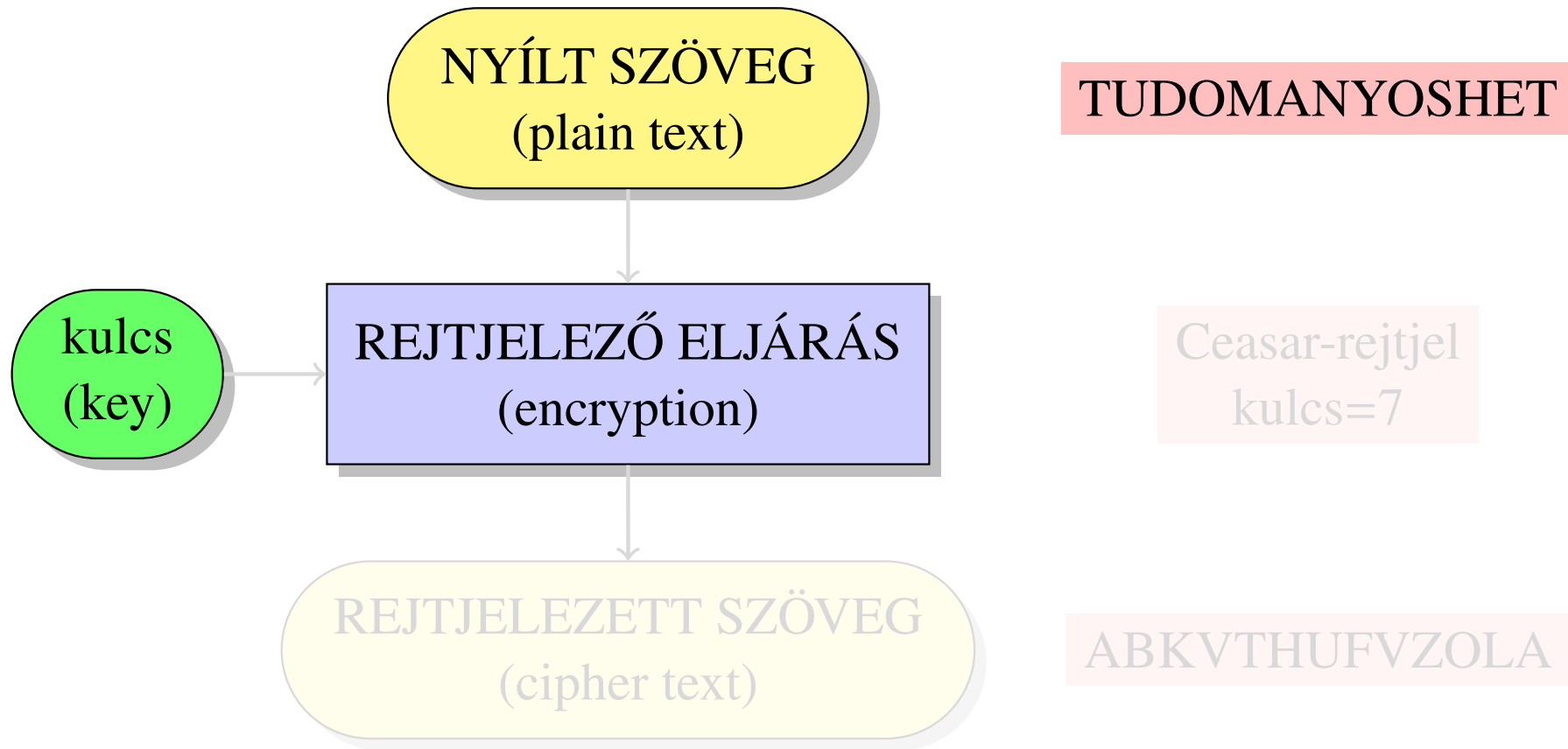
A kriptorendszer alapfogalmai: Rejtjelezés



A kriptorendszer kulcsterének fogalma

A kriptorendszer olyan kulcsainak halmaza, amik lényegesen különböző rejtjelezett szövegeket eredményeznek.

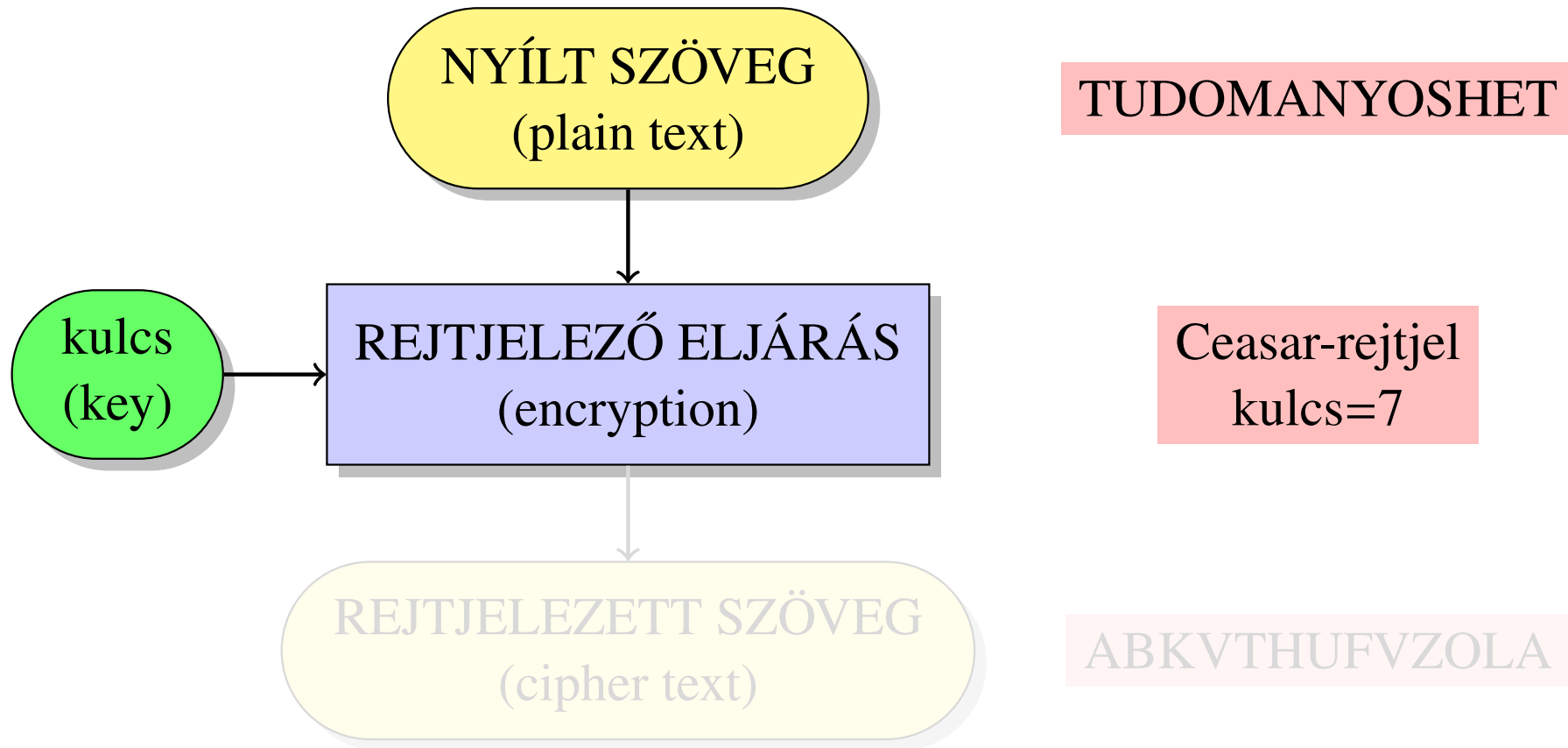
A kriptorendszer alapfogalmai: Rejtjelezés



A kriptorendszer kulcsterének fogalma

A kriptorendszer olyan kulcsainak halmaza, amik lényegesen különböző rejtjelezett szövegeket eredményeznek.

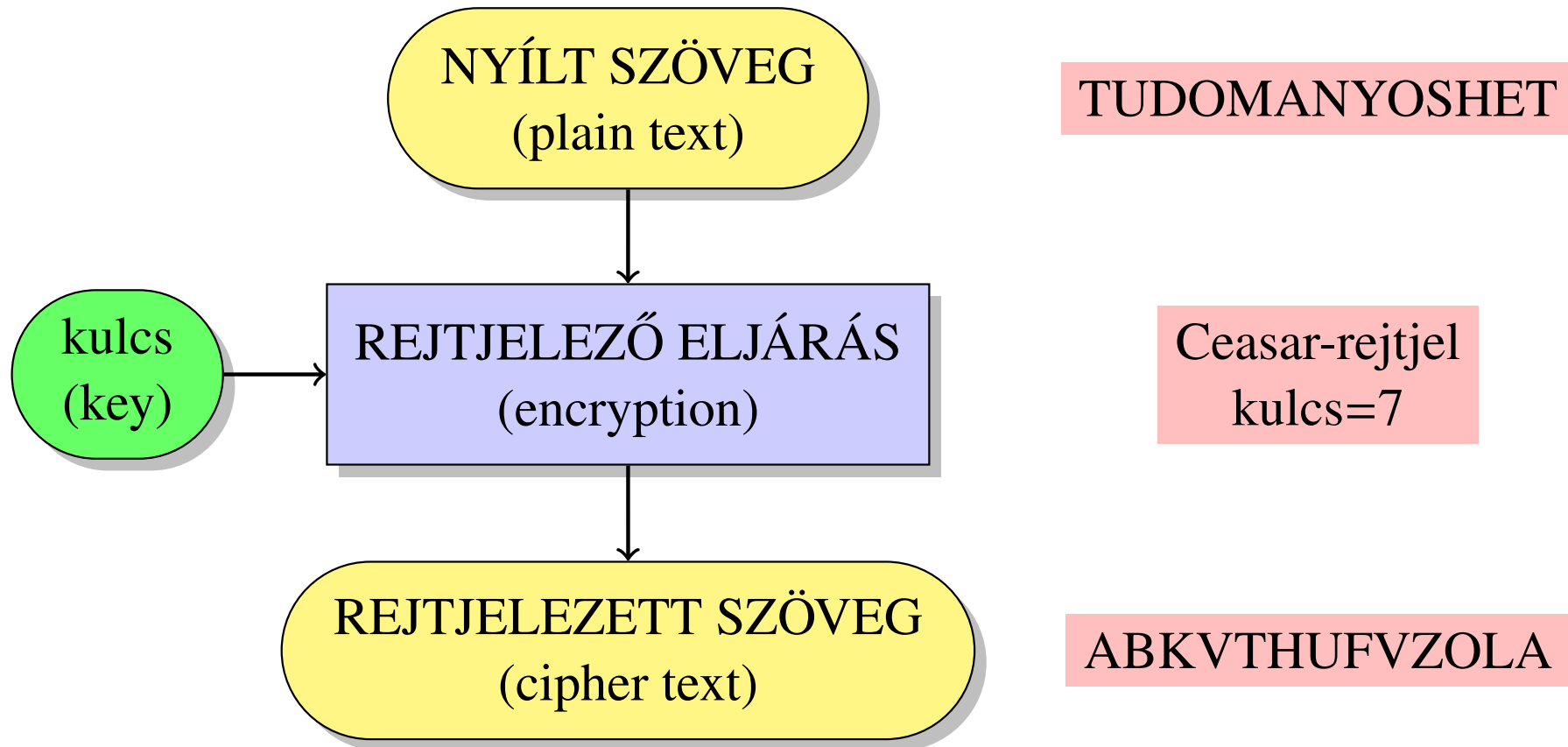
A kriptorendszer alapfogalmai: Rejtjelezés



A kriptorendszer kulcsterének fogalma

A kriptorendszer olyan kulcsainak halmaza, amik lényegesen különböző rejtjelezett szövegeket eredményeznek.

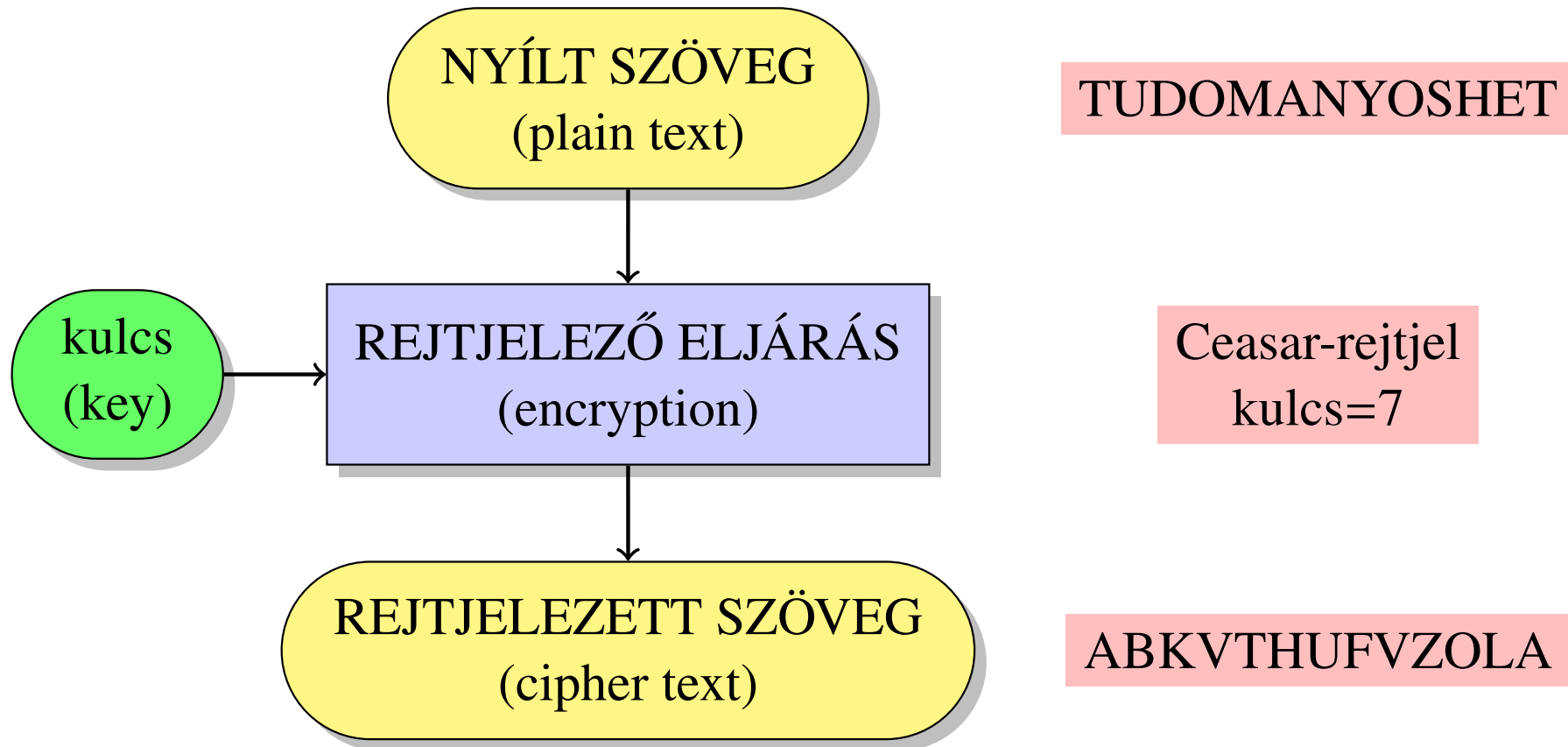
A kriptorendszer alapfogalmai: Rejtjelezés



A kriptorendszer **kulcsterének** fogalma

A kriptorendszer olyan **kulcsainak halmaza**, amik lényegesen különböző rejtjelezett szövegeket eredményeznek.

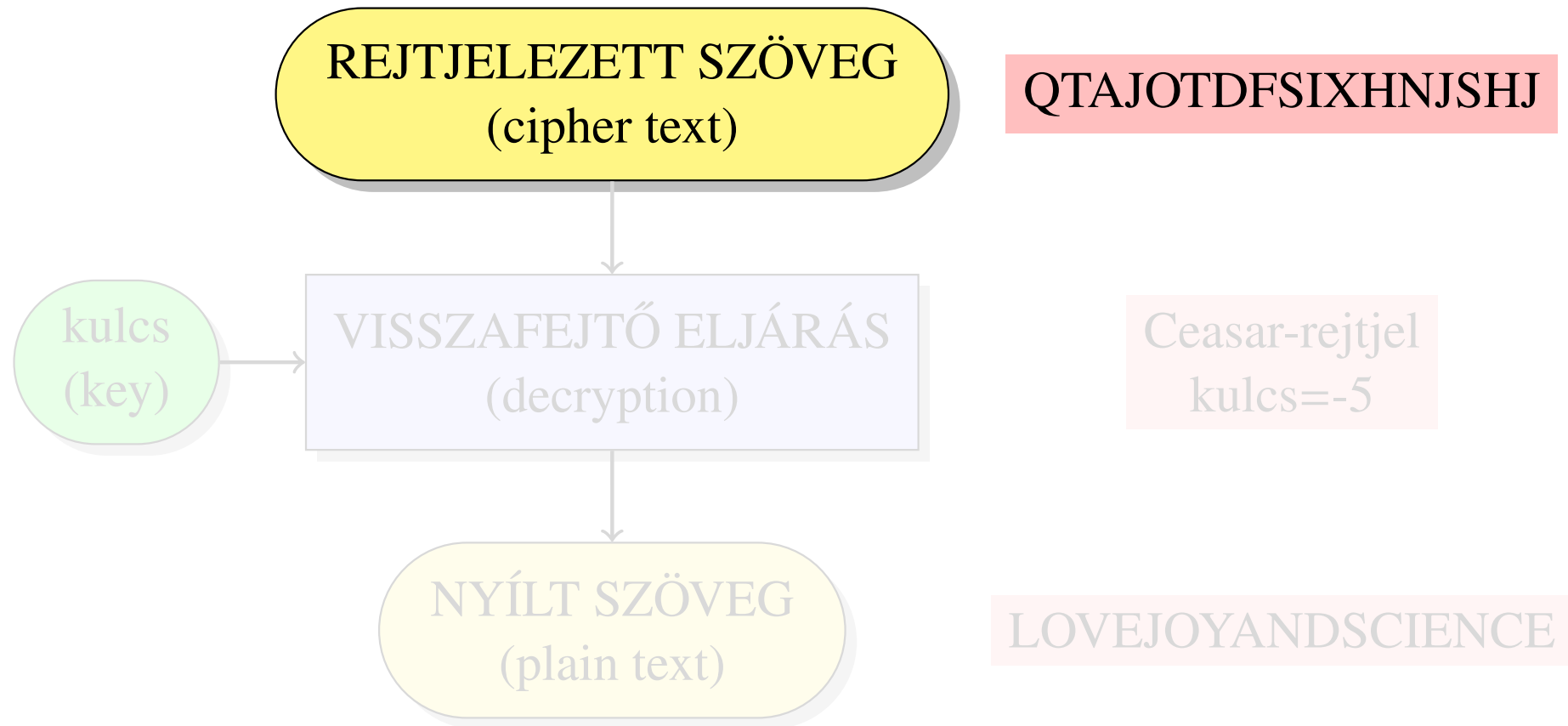
A kriptorendszer alapfogalmai: Rejtjelezés



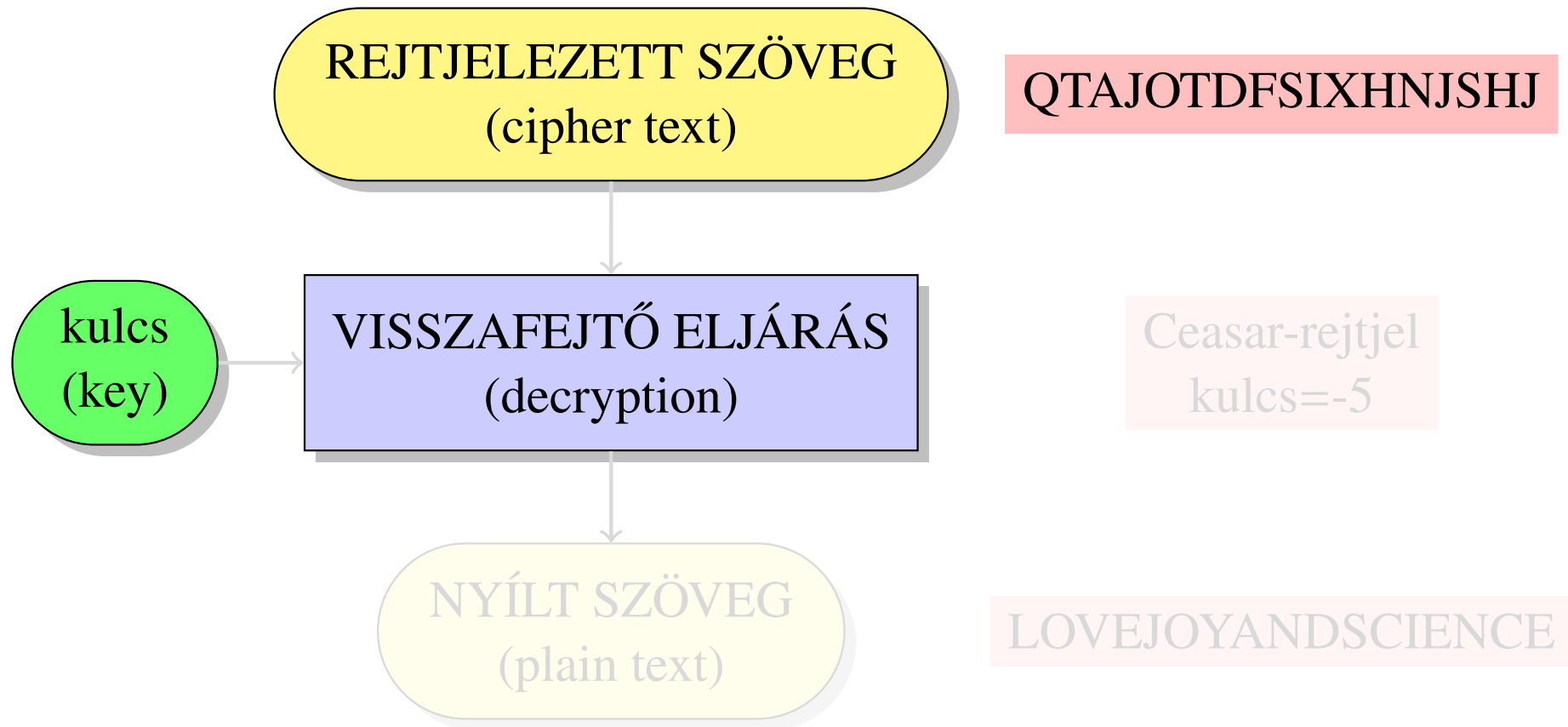
A kriptorendszer kulcsterének fogalma

A kriptorendszer olyan **kulcsainak halmaza**, amik lényegesen különböző rejtjelezett szövegeket eredményeznek.

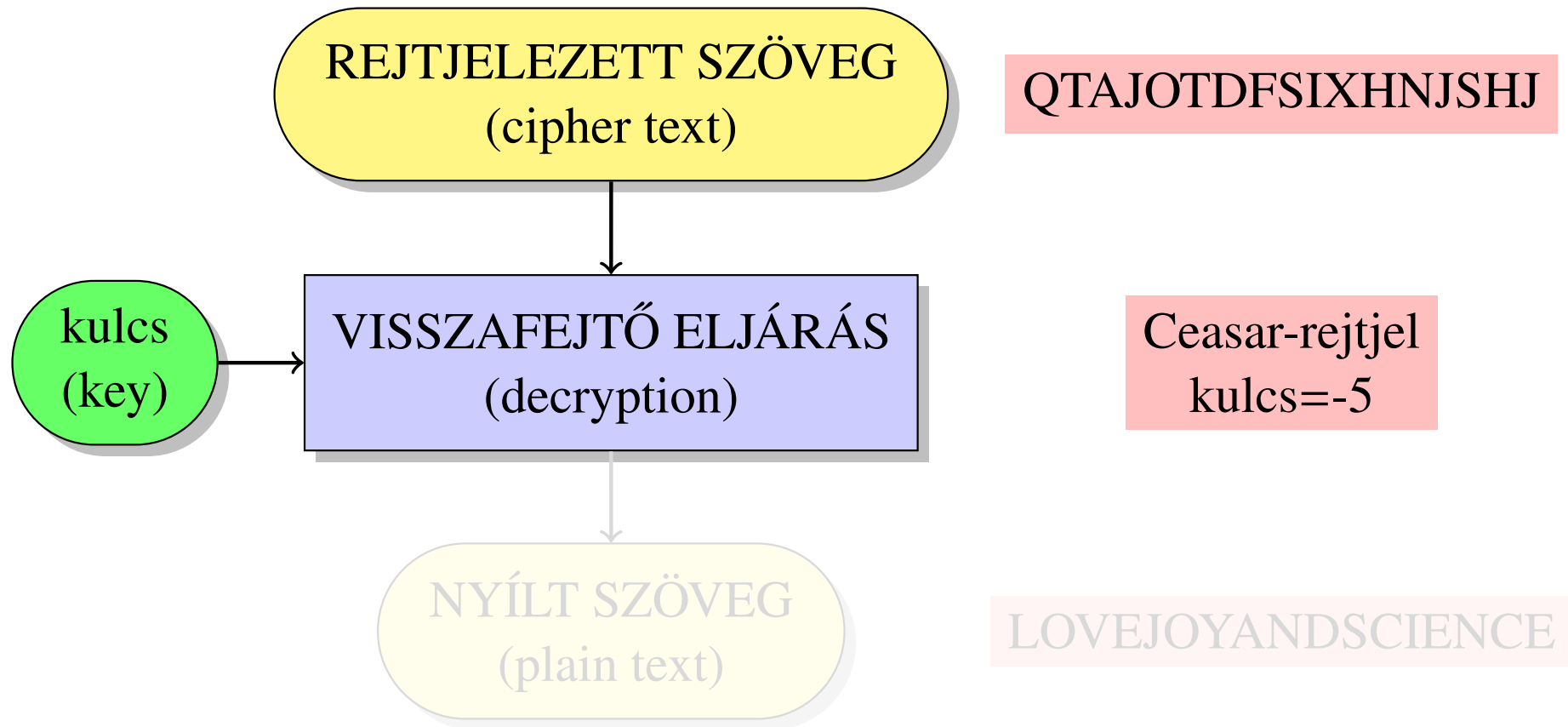
A kriptorendszer alapfogalmai: Visszafejtés



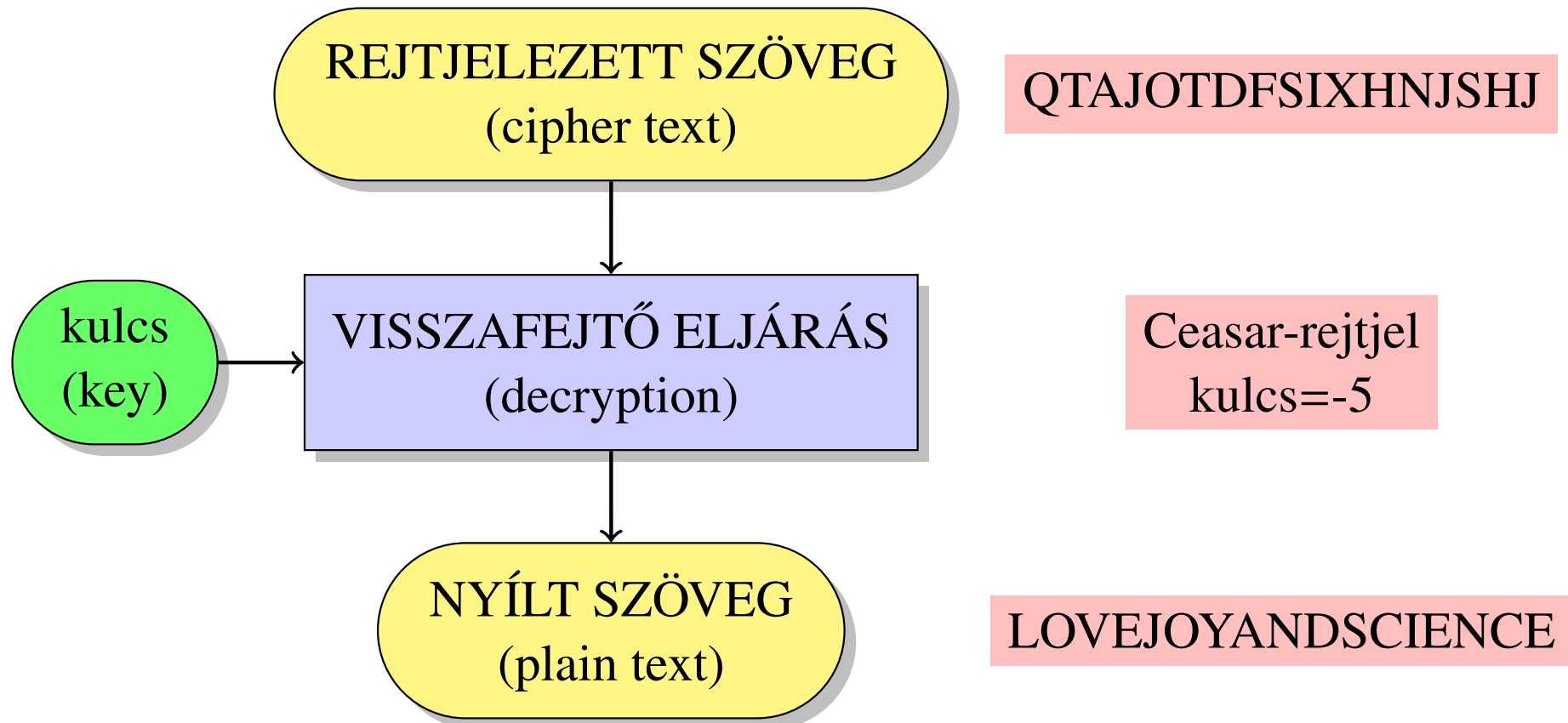
A kriptorendszer alapfogalmai: Visszafejtés



A kriptorendszer alapfogalmai: Visszafejtés



A kriptorendszer alapfogalmai: Visszafejtés



A Ceasar-féle titkosítás rendszer

- Tegyük fel, hogy a **26 betűs angol ábécét** használjuk.
- Kulcsként válasszunk egy számot **1 és 25 között**.
- Ebben a példában legyen a kulcs a **7-es**.
- A nyílt szöveg minden betűjét helyettesítsük azzal a betűvel, ami az **ábécében 7-el utána** van: $A \mapsto H$, $B \mapsto I$, stb.

1	2	3	4	5	6	7	8	9	10	...	24	25	26
A	B	C	D	E	F	G	H	I	J	...	X	Y	Z
H	I	J	K	L	M	N	O	P	Q	...	E	F	G

Sebezhetőségek

- A kulcstér csak **25 elemű**.
- Ha ismerjük **egyetlen betű megfejtését**, akkor ismerjük a kulcsot.

A Ceasar-féle titkosítás rendszer

- Tegyük fel, hogy a **26 betűs angol ábécét** használjuk.
- Kulcsként válasszunk egy számot **1 és 25 között**.
- Ebben a példában legyen a kulcs a **7-es**.
- A nyílt szöveg minden betűjét helyettesítsük azzal a betűvel, ami az **ábécében 7-el utána** van: $A \mapsto H$, $B \mapsto I$, stb.

1	2	3	4	5	6	7	8	9	10	...	24	25	26
A	B	C	D	E	F	G	H	I	J	...	X	Y	Z
H	I	J	K	L	M	N	O	P	Q	...	E	F	G

Sebezhetőségek

- A kulcstér csak **25 elemű**.
- Ha ismerjük **egyetlen betű megfejtését**, akkor ismerjük a kulcsot.

A Ceasar-rendszer „javításai”

A klasszikus monoalfabetikus rendszer

- Az ábécé ciklikus eltolásai helyett a betűk **tetszőleges összecserélése**.
- A kapott kulcstér mérete angol ábécé esetén

$$26! = 403\,291\,461\,126\,605\,635\,584\,000\,000 \approx 4 \cdot 10^{26}$$

- A ma legjobb szuperszámítógép **kb. 370 év alatt** végez ennyi műveletet.
- **Sebezhetőség:** A természetes nyelvekben a **betűk a gyakoriságuk alapján** beazonosíthatók.

Vigenère-rejtjel: A klasszikus polialfabetikus rendszer

- A Ceasar-kulcs értéke **függ a betű helyétől**.
- **Sebezhetőség:** Fejlett *statisztikai módszerek*, illetve *ismert szövegrészek*.

Ajánlott irodalom

- Edgar Allan Poe: Az aranybogár (1843)
- Verne Gyula: Nyolcszáz mérföld az Amazonason (1881)

A Kerckhoffs-féle alapelvek és a „katasztrófaforgatókönyv”

AUGUSTE KERCKHOFFS, *La Cryptographie Militaire*, 1883

- 1 A rendszernek gyakorlatilag, sőt lehetőleg matematikailag is **visszafejthetetlennek** kell lennie. A **rendszer maga nem lehet titkos**, nem jelenthet problémát, ha azt ismeri az ellenség.
- 2 A kulcsnak rövidnek és könnyen továbbíthatónak kell lenni, írott jegyzetek használata nélkül is.
- 3 A rendszer legyen használható a **Morse-távírós** kommunikációban.
- 4 A rendszernek **hordozhatónak** kell lennie, egy személy is tudja üzemelni.

A modern „katasztrófaforgatókönyv” feltételezései

- 1 Az ellenfél **teljesen ismeri** a kriptorendszerünket.
- 2 Az ellenfél **el tudja olvasni** az összes rejtjelezett szövegünket.
- 3 Az ellenfél ismeri **jelentős mennyiségű** rejtjelezett szövegünkhöz tartozó nyílt szövegünket.

A Kerckhoffs-féle alapelvek és a „katasztrófaforgatókönyv”

AUGUSTE KERCKHOFFS, *La Cryptographie Militaire*, 1883

- 1 A rendszernek gyakorlatilag, sőt lehetőleg matematikailag is **visszafejthetetlennek** kell lennie. A **rendszer maga nem lehet titkos**, nem jelenthet problémát, ha azt ismeri az ellenség.
- 2 A **kulcsnak rövidnek és könnyen továbbíthatónak** kell lenni, írott jegyzetek használata nélkül is.
- 3 A rendszer legyen használható a **Morse-távírós** kommunikációban.
- 4 A rendszernek **hordozhatónak** kell lennie, egy személy is tudja üzemelni.

A modern „katasztrófaforgatókönyv” feltételezései

- 1 Az ellenfél **teljesen ismeri** a kriptorendszerünket.
- 2 Az ellenfél **el tudja olvasni** az összes rejtjelezett szövegünket.
- 3 Az ellenfél ismeri **jelentős mennyiségű** rejtjelezett szövegünkhöz tartozó nyílt szövegünket.

A Kerckhoffs-féle alapelvek és a „katasztrófaforgatókönyv”

AUGUSTE KERCKHOFFS, *La Cryptographie Militaire*, 1883

- 1 A rendszernek gyakorlatilag, sőt lehetőleg matematikailag is **visszafejthetetlennek** kell lennie. A **rendszer maga nem lehet titkos**, nem jelenthet problémát, ha azt ismeri az ellenség.
- 2 A **kulcsnak rövidnek és könnyen továbbíthatónak** kell lenni, írott jegyzetek használata nélkül is.
- 3 A rendszer legyen használható a **Morse-távírós** kommunikációban.
- 4 A rendszernek **hordozhatónak** kell lennie, egy személy is tudja üzemelni.

A modern „katasztrófaforgatókönyv” feltételezései

- Az ellenfél **teljesen ismeri** a kriptorendszerünket.
- Az ellenfél **el tudja olvasni** az összes rejtjelezett szövegünket.
- Az ellenfél ismeri **jelentős mennyiségű** rejtjelezett szövegünkhöz tartozó nyílt szövegünket.

A Kerckhoffs-féle alapelvek és a „katasztrófaforgatókönyv”

AUGUSTE KERCKHOFFS, *La Cryptographie Militaire*, 1883

- 1 A rendszernek gyakorlatilag, sőt lehetőleg matematikailag is **visszafejthetetlennek** kell lennie. A **rendszer maga nem lehet titkos**, nem jelenthet problémát, ha azt ismeri az ellenség.
- 2 A **kulcsnak rövidnek és könnyen továbbíthatónak** kell lenni, írott jegyzetek használata nélkül is.
- 3 A rendszer legyen használható a **Morse-távírós** kommunikációban.
- 4 A rendszernek **hordozhatónak** kell lennie, egy személy is tudja üzemelni.

A modern „katasztrófaforgatókönyv” feltételezései

- Az ellenfél **teljesen ismeri** a kriptorendszerünket.
- Az ellenfél **el tudja olvasni** az összes rejtjelezett szövegünket.
- Az ellenfél ismeri **jelentős mennyiségű** rejtjelezett szövegünkhöz tartozó nyílt szövegünket.

A Kerckhoffs-féle alapelvek és a „katasztrófaforgatókönyv”

AUGUSTE KERCKHOFFS, *La Cryptographie Militaire*, 1883

- 1 A rendszernek gyakorlatilag, sőt lehetőleg matematikailag is **visszafejthetetlennek** kell lennie. A **rendszer maga nem lehet titkos**, nem jelenthet problémát, ha azt ismeri az ellenség.
- 2 A **kulcsnak rövidnek és könnyen továbbíthatónak** kell lenni, írott jegyzetek használata nélkül is.
- 3 A rendszer legyen használható a **Morse-távírós** kommunikációban.
- 4 A rendszernek **hordozhatónak** kell lennie, egy személy is tudja üzemelni.

A modern „katasztrófaforgatókönyv” feltételezései

- Az ellenfél **teljesen ismeri** a kriptorendszerünket.
- Az ellenfél **el tudja olvasni** az összes rejtjelezett szövegünket.
- Az ellenfél ismeri **jelentős mennyiségű** rejtjelezett szövegünkhöz tartozó nyílt szövegünket.

A Kerckhoffs-féle alapelvek és a „katasztrófaforgatókönyv”

AUGUSTE KERCKHOFFS, *La Cryptographie Militaire*, 1883

- 1 A rendszernek gyakorlatilag, sőt lehetőleg matematikailag is **visszafejthetetlennek** kell lennie. A **rendszer maga nem lehet titkos**, nem jelenthet problémát, ha azt ismeri az ellenség.
- 2 A **kulcsnak rövidnek és könnyen továbbíthatónak** kell lenni, írott jegyzetek használata nélkül is.
- 3 A rendszer legyen használható a **Morse-távírós** kommunikációban.
- 4 A rendszernek **hordozhatónak** kell lennie, egy személy is tudja üzemelni.

A modern „katasztrófaforgatókönyv” feltételezései

- 1 Az ellenfél **teljesen ismeri** a kriptorendszerünket.
- 2 Az ellenfél el tudja olvasni az **összes rejtjelezett szövegünket**.
- 3 Az ellenfél ismeri **jelentős mennyiségű** rejtjelezett szövegünkhöz tartozó **nyílt szövegünket**.

A Kerckhoffs-féle alapelvek és a „katasztrófaforgatókönyv”

AUGUSTE KERCKHOFFS, *La Cryptographie Militaire*, 1883

- 1 A rendszernek gyakorlatilag, sőt lehetőleg matematikailag is **visszafejthetetlennek** kell lennie. A **rendszer maga nem lehet titkos**, nem jelenthet problémát, ha azt ismeri az ellenség.
- 2 A **kulcsnak rövidnek és könnyen továbbíthatónak** kell lenni, írott jegyzetek használata nélkül is.
- 3 A rendszer legyen használható a **Morse-távírós** kommunikációban.
- 4 A rendszernek **hordozhatónak** kell lennie, egy személy is tudja üzemelni.

A modern „katasztrófaforgatókönyv” feltételezései

- 1 Az ellenfél **teljesen ismeri** a kriptorendszerünket.
- 2 Az ellenfél el tudja olvasni az **összes rejtjelezett szövegünket**.
- 3 Az ellenfél ismeri **jelentős mennyiségű** rejtjelezett szövegünkhöz tartozó **nyílt szövegünket**.

A Kerckhoffs-féle alapelvek és a „katasztrófaforgatókönyv”

AUGUSTE KERCKHOFFS, *La Cryptographie Militaire*, 1883

- 1 A rendszernek gyakorlatilag, sőt lehetőleg matematikailag is **visszafejthetetlennek** kell lennie. A **rendszer maga nem lehet titkos**, nem jelenthet problémát, ha azt ismeri az ellenség.
- 2 A **kulcsnak rövidnek és könnyen továbbíthatónak** kell lenni, írott jegyzetek használata nélkül is.
- 3 A rendszer legyen használható a **Morse-távírós** kommunikációban.
- 4 A rendszernek **hordozhatónak** kell lennie, egy személy is tudja üzemelni.

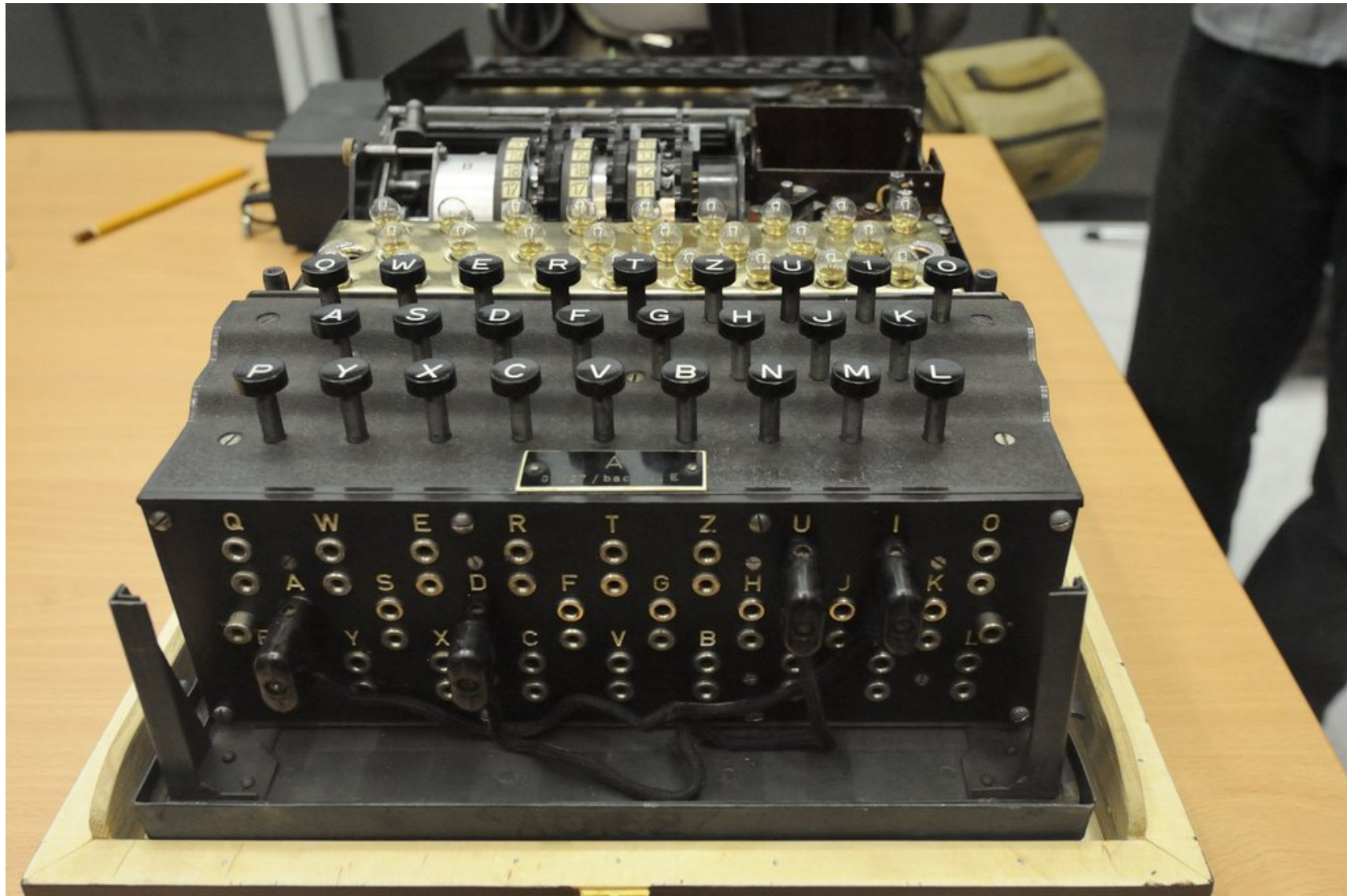
A modern „katasztrófaforgatókönyv” feltételezései

- 1 Az ellenfél **teljesen ismeri** a kriptorendszerünket.
- 2 Az ellenfél el tudja olvasni az **összes rejtjelezett szövegünket**.
- 3 Az ellenfél ismeri **jelentős mennyiségű** rejtjelezett szövegünkhöz tartozó **nyílt szövegünket**.

Table of Contents

- 1 A titkosírások elméleti alapelvei
- 2 Az Enigma-rendszerek működése**
- 3 Az Enigma sebezhetőségei
- 4 Napjaink kriptorendszerei

Az Enigma készülék



Az Enigma készülék



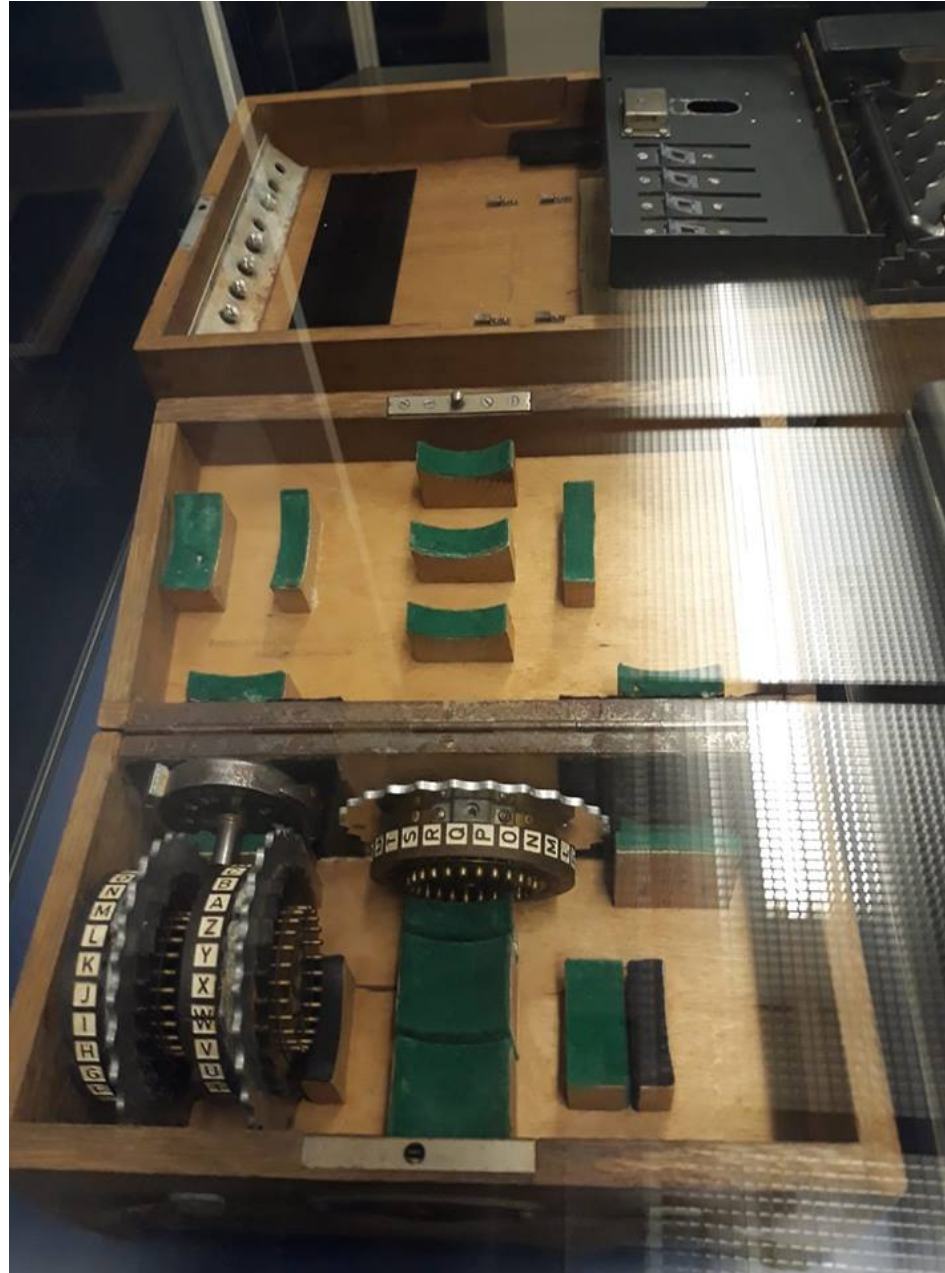
Az Enigma készülék



Az Enigma készülék



Az Enigma készülék



Az Enigma típusok

- A német hadsereg 1926-tól használt **Enigma** típusú gépeket rejtjelezésre.
- A hadsereg különböző részei (szárazföldi erők, haditengerészet, légierő, titkosszolgálatok) **különböző típusokat** használtak.
- Az évek során a típusokat **fejlesztették** is, igyekeztek növelni a titkosítás erősségét.
- Ezen a képen GUDERIAN páncélos tábornok látható 1940-ben az Enigma használata közben.



Az Enigma típusok

- A német hadsereg 1926-tól használt **Enigma** típusú gépeket rejtjelezésre.
- A hadsereg különböző részei (szárazföldi erők, haditengerészet, légierő, titkosszolgálatok) **különböző típusokat** használtak.
- Az évek során a típusokat **fejlesztették** is, igyekeztek növelni a titkosítás erősségét.
- Ezen a képen GUDERIAN páncélos tábornok látható 1940-ben az Enigma használata közben.



Az Enigma típusok

- A német hadsereg 1926-tól használt **Enigma** típusú gépeket rejtjelezésre.
- A hadsereg különböző részei (szárazföldi erők, haditengerészet, légierő, titkosszolgálatok) **különböző típusokat** használtak.
- Az évek során a típusokat **fejlesztették** is, igyekeztek növelni a titkosítás erősségét.
- Ezen a képen GUDERIAN páncélos tábornok látható 1940-ben az Enigma használata közben.



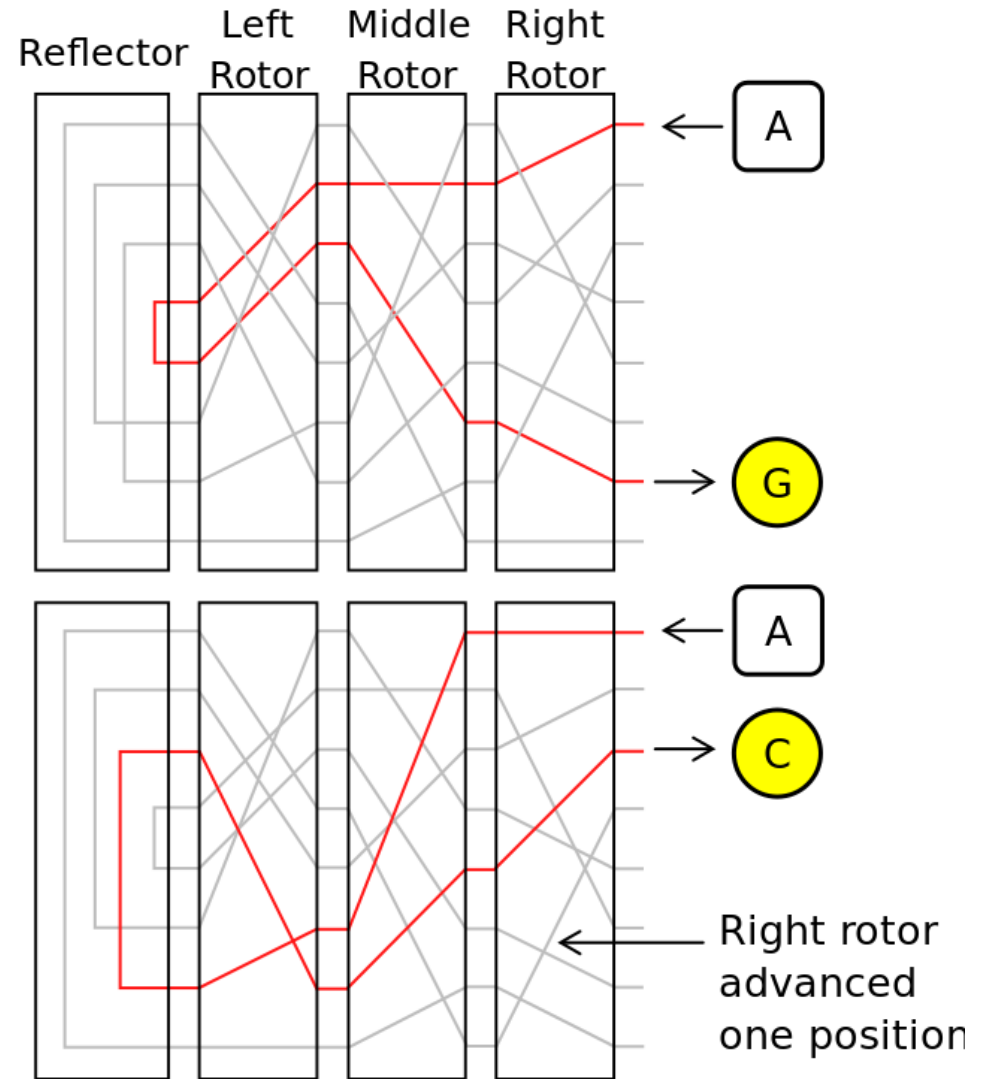
Az Enigma típusok

- A német hadsereg 1926-tól használt **Enigma** típusú gépeket rejtjelezésre.
- A hadsereg különböző részei (szárazföldi erők, haditengerészet, légierő, titkosszolgálatok) **különböző típusokat** használtak.
- Az évek során a típusokat **fejlesztették** is, igyekeztek növelni a titkosítás erősségét.
- Ezen a képen GUDERIAN páncélos tábornok látható 1940-ben az Enigma használata közben.



Az Enigma típusok közös működési alapelvei

- **Polialfabetikus** rendszer 26 ékezet nélküli latin betűs ábécével.
- **Elektromos működés** egy billentyűzet és egy lámpamező segítségével.
- A **kulcs** két részből tevődik össze
 - (1) 3-4 **cserélhető forgótárcsa** és egy **visszafordító tárcsa** (*Walzen*)
 - (2) **Kapocstábla** 10 pár csatlakozó dugóval (*Steckerbrett*)



Enigma demó programok

- Böngészőben futó program, grafikus demó beállításokkal:
<https://www.101computing.net/enigma-machine-emulator/>
- Android program tabletre és okostelefonra, grafikus demó beállításokkal:
Enigma Simulator Franklin Heath Ltd

Az Enigma használata

- Minden napra volt egy előre meghatározott **napi kulcs**, ami tartalmazta a tárcsák és a kapocstábla **kezdeti beállításait**.
- A napi kulcsokat **havonta** előre kiadták egy szigorúan titkos kiadványban. (A tengeralattjárókon *vízben oldható* papírral-tintával.)

Geheim!
Nicht im Flugzeug mitnehmen!

Sonder-Maschinenschlüssel BGT

Datum	Wahrsage	Flagstellung	Stecherverbindungen														Kettengruppe		
21.	I V III	06 20 24	UA	PF	RQ	SO	NI	EY	BO	HL	TX	ZJ					jou	nyq	aqm
20.	V II III	01 07 12	GF	KV	JM	IB	UW	LX	TD	QS	NA	2H					ass	zds	kek
29.	IV I V	11 17 26	CI	OK	PV	ZL	HX	NB	AW	DJ	FE	ST					kap	gwh	lyx

- Egy üzenet **maximum 250 karakterből** állhatott.
- **Minden üzenetnek külön kulcsa** volt, **egyéni tárcsabeállítással**; a napi kapocstábla beállítást nem változtatták.
- Az üzenet **fejlécében** közölték az egyéni tárcsabeállítást.
- Az üzenteket **Morse-jelekkel** rádióon továbbították.

Példa: Egy eredeti rejtjelezett Enigma-üzenet

H6R 5RH DE C 1346 = 3TLE = 2TL 224 = HUW XNG =
 DKRKI CUZAF MNSDC AWXVJ DVZNH DMOZN NWRJC KKJQO
 ELWIK XDUUF ^RECEGN OUNNQ CIIZX ^NFUTOF BTNWI GOECK
 CMYUC KTTYB ZMDTU WCNWH OXOFX ERVQW JUCVY PQACQ
 EBMXE NOQKF LWRWR LGKXZ BPYWR GQVYG WJDGA QXKVC
 MQQJJ PVSLG WFZJZ HHWQG YFCQQ RMVRR QQIDQ QVVIW
 LJLBH LHHD1 OFWUY JJQG X BWPZ

Példa: Egy eredeti rejtjelezett Enigma-üzenet

fejléc

H6R 5RH DE C 1346 = 3TLE = 2TL 224 = HUW XNG =

DKRKI	CUZAF	MNSDC	AWXVJ	DVZNH	DMOZN	NWRJC	KKJQO
ELWIK	XDUUF	ECEGN	OUNNQ	CIIZX	FUTOF	BTNWI	GOECK
CMYUC	KTTYB	ZMDTU	WCNWH	OXOFX	ERVQW	JUCVY	PQACQ
EBMXE	NOQKF	LWRWR	LGKXZ	BPYWR	GQVYG	WJDGA	QXKVC
MQQJJ	PVSLG	WFZJZ	HHWQG	YFCQQ	RMVRR	QQIDQ	QVVIW
LJLBH	LHHD1	OFWUY	JJQG X	BWPZ			

Példa: Egy eredeti rejtjelezett Enigma-üzenet

fejléc

karakterszám

H6R 5RH DE C 1346 = 3TLE = 2TL 224 = HUW XNG =
 DKRKI CUZAF MNSDC AWXVJ DVZNH DMOZN NWRJC KKJQO
 ELWIK XDUUF ECEGN OUNNQ CIIZX FUTOF BTNWI GOECK
 CMYUC KTTYB ZMDTU WCNWH OXOFX ERVQW JUCVY PQACQ
 EBMXE NOQKF LWRWR LGKXZ BPYWR GQVYG WJDGA QXKVC
 MQQJJ PVSLG WFZJZ HHWQG YFCQQ RMVRR QQIDQ QVVIW
 LJLBH LHHD1 OFWUY JJQG X BWPZ

Példa: Egy eredeti rejtjelezett Enigma-üzenet

fejléc

egyedi tárcsa állás

H6R 5RH DE C 1346 = 3TLE = 2TL 224 = HUW XNG =

DKRKI	CUZAF	MNSDC	AWXVJ	DVZNH	DMOZN	NWRJC	KKJQO
ELWIK	XDUUF	ECEGN	OUNNQ	CIIZX	FUTOF	BTNWI	GOECK
CMYUC	KTTYB	ZMDTU	WCNWH	OXOFX	ERVQW	JUCVY	PQACQ
EBMXE	NOQKF	LWRWR	LGKXZ	BPYWR	GQVYG	WJDGA	QXKVC
MQQJJ	PVSLG	WFZJZ	HHWQG	YFCQQ	RMVRR	QQIDQ	QVVIW
LJLBH	LHHD1	OFWUY	JJQGX	BWPZ			

Az Enigma I kulcsstere

- A rendelkezésre álló 5 tárcsából 3-at kell a megfelelő helyre beilleszteni:
 $5 \cdot 4 \cdot 3 = 60$ lehetőség.
- A három tárcsának $26^3 = 17\,576$ állása van.
- A 26 betűből 10 párat összeállítani a kapocstáblán

$$\frac{26!}{2^{10} \cdot 10! \cdot 6!} = 150\,738\,274\,937\,250$$

féleképpen lehet.

- Ez összesen

$$158\,962\,555\,217\,826\,360\,000 \approx 1,59 \cdot 10^{20} \approx 2^{67}.$$

- Ez a Kódjatszma c. filmben elhangzó „150 millió millió millió”.
- A **kulcsstér mérete** miatt az Enigmát a szakemberek egybehangzóan **feltörhetetlennek tartották.**

Table of Contents

- 1 A titkosírások elméleti alapelvei
- 2 Az Enigma-rendszerek működése
- 3 Az Enigma sebezhetőségei**
- 4 Napjaink kriptorendszerei

Az Enigma-rendszerek sebezhetőségei

Kis hibák:

- Titokban akarták tartani a **tárcsák drótozását**.
- Végig **ugyanazt a 8 tárcsát** használták.
- Az Enigma I változatnál (1940-ig) az üzenet egyéni kulcsát (3 tárcsa állása, pl. **GTA**) **duplán megismételve** küldték el (pl. **UZH PKL**).
- Ez azt jelenti, hogy az üzenet **1. és 4., 2. és 5. valamint 3. és 6. betűje ugyanazt a betűt** rejtjelezik.
- Ez nagyon durván **lecsökkentette a kulcstér méretét**.

Nagy hibák:

- Rengeteg sablonos német üzenet katonás rendben, pl. **napi időjárás jelentések**.
- A gép minden beállítása a 26 betű egy *fixpontmentes involutórikus permutációját* hozza létre, azaz
 - (1) ha pl. az **U betű rejtjele a C**, akkor a **C betűé az U**,
 - (2) és **egyetlen betű sem egyezhet meg a rejtjelével**.

Az Enigma-rendszerek sebezhetőségei

Kis hibák:

- Titokban akarták tartani a **tárcsák drótozását**.
- Végig **ugyanazt a 8 tárcsát** használták.
- Az Enigma I változatnál (1940-ig) az üzenet egyéni kulcsát (3 tárcsa állása, pl. **GTA**) **duplán megismételve** küldték el (pl. **UZH PKL**).
- Ez azt jelenti, hogy az üzenet **1. és 4., 2. és 5. valamint 3. és 6. betűje ugyanazt a betűt** rejtjelezik.
- Ez nagyon durván **lecsökkentette a kulcstér méretét**.

Nagy hibák:

- Rengeteg sablonos német üzenet katonás rendben, pl. **napi időjárás jelentések**.
- A gép minden beállítása a 26 betű egy *fixpontmentes involutórikus permutációját* hozza létre, azaz
 - (1) ha pl. az U betű rejtjele a C, akkor a C betűé az U,
 - (2) és egyetlen betű sem egyezhet meg a rejtjelével.

Az Enigma-rendszerek sebezhetőségei

Kis hibák:

- Titokban akarták tartani a **tárcsák drótozását**.
- Végig **ugyanazt a 8 tárcsát** használták.
- Az Enigma I változatnál (1940-ig) az üzenet egyéni kulcsát (3 tárcsa állása, pl. **GTA**) **duplán megismételve** küldték el (pl. **UZT PKL**).
- Ez azt jelenti, hogy az üzenet **1. és 4., 2. és 5. valamint 3. és 6. betűje ugyanazt a betűt** rejtjelezik.
- Ez nagyon durván **lecsökkentette a kulcstér méretét**.

Nagy hibák:

- Rengeteg sablonos német üzenet katonás rendben, pl. **napi időjárás jelentések**.
- A gép minden beállítása a 26 betű egy *fixpontmentes involutórikus permutációját* hozza létre, azaz
 - (1) ha pl. az U betű rejtjele a C, akkor a C betűé az U,
 - (2) és egyetlen betű sem egyezhet meg a rejtjelével.

Az Enigma-rendszerek sebezhetőségei

Kis hibák:

- Titokban akarták tartani a **tárcsák drótozását**.
- Végig **ugyanazt a 8 tárcsát** használták.
- Az Enigma I változatnál (1940-ig) az üzenet egyéni kulcsát (3 tárcsa állása, pl. **GTA**) **duplán megismételve** küldték el (pl. **UZT PKL**).
- Ez azt jelenti, hogy az üzenet **1. és 4., 2. és 5. valamint 3. és 6. betűje ugyanazt a betűt** rejtjelezik.
- Ez nagyon durván **lecsökkentette a kulcstér méretét**.

Nagy hibák:

- Rengeteg sablonos német üzenet katonás rendben, pl. **napi időjárás jelentések**.
- A gép minden beállítása a 26 betű egy *fixpontmentes involutórikus permutációját* hozza létre, azaz
 - (1) ha pl. az U betű rejtjele a C, akkor a C betűé az U,
 - (2) és egyetlen betű sem egyezhet meg a rejtjelével.

Az Enigma-rendszerek sebezhetőségei

Kis hibák:

- Titokban akarták tartani a **tárcsák drótozását**.
- Végig **ugyanazt a 8 tárcsát** használták.
- Az Enigma I változatnál (1940-ig) az üzenet egyéni kulcsát (3 tárcsa állása, pl. **GTA**) **duplán megismételve** küldték el (pl. **UZT PKL**).
- Ez azt jelenti, hogy az üzenet **1. és 4., 2. és 5.** valamint **3. és 6.** betűje **ugyanazt a betűt** rejtjelezi.
- Ez nagyon durván **lecsökkentette a kulcstér méretét**.

Nagy hibák:

- Rengeteg sablonos német üzenet katonás rendben, pl. napi időjárás jelentések.
- A gép minden beállítása a 26 betű egy *fixpontmentes involutórikus permutációját* hozza létre, azaz
 - (1) ha pl. az U betű rejtjele a C, akkor a C betűé az U,
 - (2) és egyetlen betű sem egyezhet meg a rejtjelével.

Az Enigma-rendszerek sebezhetőségei

Kis hibák:

- Titokban akarták tartani a **tárcsák drótozását**.
- Végig **ugyanazt a 8 tárcsát** használták.
- Az Enigma I változatnál (1940-ig) az üzenet egyéni kulcsát (3 tárcsa állása, pl. **GTA**) **duplán megismételve** küldték el (pl. **UZT PKL**).
- Ez azt jelenti, hogy az üzenet **1. és 4., 2. és 5.** valamint **3. és 6.** betűje **ugyanazt a betűt** rejtjelezi.
- Ez nagyon durván **lecsökkentette a kulcstér méretét**.

Nagy hibák:

- Rengeteg sablonos német üzenet katonás rendben, pl. napi időjárás jelentések.
- A gép minden beállítása a 26 betű egy *fixpontmentes involutórikus permutációját* hozza létre, azaz
 - (1) ha pl. az U betű rejtjele a C, akkor a C betűé az U,
 - (2) és egyetlen betű sem egyezhet meg a rejtjelével.

Az Enigma-rendszerek sebezhetőségei

Kis hibák:

- Titokban akarták tartani a **tárcsák drótozását**.
- Végig **ugyanazt a 8 tárcsát** használták.
- Az Enigma I változatnál (1940-ig) az üzenet egyéni kulcsát (3 tárcsa állása, pl. **GTA**) **duplán megismételve** küldték el (pl. **UZT PKL**).
- Ez azt jelenti, hogy az üzenet **1. és 4., 2. és 5. valamint 3. és 6. betűje ugyanazt a betűt** rejtjelezik.
- Ez nagyon durván **lecsökkentette a kulcstér méretét**.

Nagy hibák:

- Rengeteg sablonos német üzenet katonás rendben, pl. **napi időjárás jelentések**.
- A gép minden beállítása a 26 betű egy *fixpontmentes involutórikus permutációját* hozza létre, azaz
 - (1) ha pl. az **U betű rejtjele a C**, akkor a **C betűé az U**,
 - (2) és **egyetlen betű sem egyezhet meg a rejtjelével**.

Az Enigma-rendszerek sebezhetőségei

Kis hibák:

- Titokban akarták tartani a **tárcsák drótozását**.
- Végig **ugyanazt a 8 tárcsát** használták.
- Az Enigma I változatnál (1940-ig) az üzenet egyéni kulcsát (3 tárcsa állása, pl. **GTA**) **duplán megismételve** küldték el (pl. **UZT PKL**).
- Ez azt jelenti, hogy az üzenet **1. és 4., 2. és 5. valamint 3. és 6. betűje ugyanazt a betűt** rejtjelezik.
- Ez nagyon durván **lecsökkentette a kulcstér méretét**.

Nagy hibák:

- Rengeteg sablonos német üzenet katonás rendben, pl. **napi időjárás jelentések**.
- A gép minden beállítása a 26 betű egy *fixpontmentes involutórikus permutációját* hozza létre, azaz
 - (1) ha pl. az **U betű rejtjele a C**, akkor a **C betűé az U**,
 - (2) és **egyetlen betű sem egyezhet meg a rejtjelével**.

Az Enigma-rendszerek sebezhetőségei

Kis hibák:

- Titokban akarták tartani a **tárcsák drótozását**.
- Végig **ugyanazt a 8 tárcsát** használták.
- Az Enigma I változatnál (1940-ig) az üzenet egyéni kulcsát (3 tárcsa állása, pl. **GTA**) **duplán megismételve** küldték el (pl. **UZT PKL**).
- Ez azt jelenti, hogy az üzenet **1. és 4., 2. és 5.** valamint **3. és 6.** betűje **ugyanazt a betűt** rejtjelezi.
- Ez nagyon durván **lecsökkentette a kulcstér méretét**.

Nagy hibák:

- Rengeteg sablonos német üzenet katonás rendben, pl. **napi időjárás jelentések**.
- A gép minden beállítása a 26 betű egy *fixpontmentes involutórikus permutációját* hozza létre, azaz
 - (1) ha pl. az **U betű rejtjele a C**, akkor a **C betűé az U**,
 - (2) és egyetlen betű sem egyezhet meg a rejtjelével.

Az Enigma-rendszerek sebezhetőségei

Kis hibák:

- Titokban akarták tartani a **tárcsák drótozását**.
- Végig **ugyanazt a 8 tárcsát** használták.
- Az Enigma I változatnál (1940-ig) az üzenet egyéni kulcsát (3 tárcsa állása, pl. **GTA**) **duplán megismételve** küldték el (pl. **UZT PKL**).
- Ez azt jelenti, hogy az üzenet **1. és 4., 2. és 5. valamint 3. és 6. betűje ugyanazt a betűt** rejtjelezik.
- Ez nagyon durván **lecsökkentette a kulcstér méretét**.

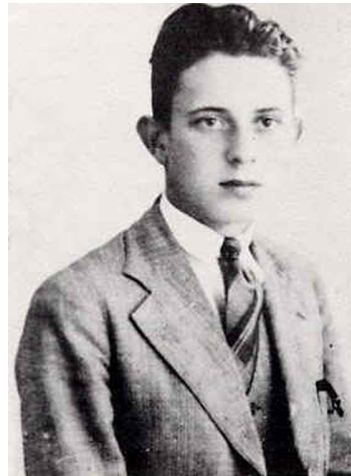
Nagy hibák:

- Rengeteg sablonos német üzenet katonás rendben, pl. **napi időjárás jelentések**.
- A gép minden beállítása a 26 betű egy *fixpontmentes involutórikus permutációját* hozza létre, azaz
 - (1) ha pl. az **U betű rejtjele a C**, akkor a **C betűé az U**,
 - (2) és **egyetlen betű sem egyezhet meg a rejtjelével**.

Az Enigma feltörése: a lengyel matematikusok munkája



MARIAN REJEWSKI



JERZY RÓŻYCKI



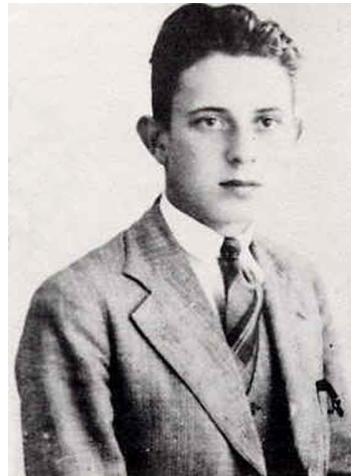
HENRYK ZYGALSKI

- Brillións **absztrakt matematikai** módszerekkel, a *véges permutációcsoportok elméletét* használva megfejtették a **tárcsák drótozását**.
- Rájöttek, hogy amennyiben a rejtjelezett szövegben **ismert szó** szerepel, azt könnyen **be lehet azonosítani** felhasználva, hogy *egyetlen betű sem rejtjelezi saját magát*.
- **Mechanikus számítógépet** építettek a megmaradó (még mindig igen nagy) kulcstér szisztematikus átvizsgálására: a **BOMBA-t**.

Az Enigma feltörése: a lengyel matematikusok munkája



MARIAN REJEWSKI



JERZY RÓŻYCKI



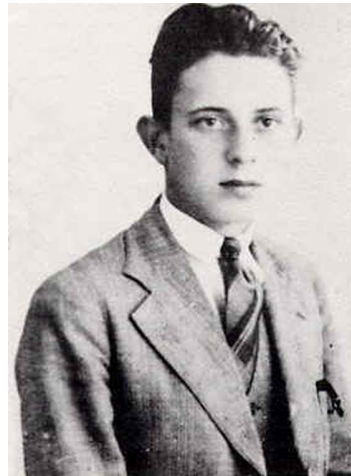
HENRYK ZYGALSKI

- Brillións **absztrakt matematikai** módszerekkel, a *véges permutációcsoportok elméletét* használva megfejtették a **tárcsák drótozását**.
- Rájöttek, hogy amennyiben a rejtjelezett szövegben **ismert szó** szerepel, azt könnyen **be lehet azonosítani** felhasználva, hogy *egyetlen betű sem rejtjelezi saját magát*.
- **Mechanikus számítógépet** építettek a megmaradó (még mindig igen nagy) kulcstér szisztematikus átvizsgálására: a **BOMBA-t**.

Az Enigma feltörése: a lengyel matematikusok munkája



MARIAN REJEWSKI



JERZY RÓŻYCKI



HENRYK ZYGALSKI

- Brillións **absztrakt matematikai** módszerekkel, a *véges permutációcsoportok elméletét* használva megfejtették a **tárcsák drótozását**.
- Rájöttek, hogy amennyiben a rejtjelezett szövegben **ismert szó** szerepel, azt könnyen **be lehet azonosítani** felhasználva, hogy *egyetlen betű sem rejtjelezi saját magát*.
- **Mechanikus számítógépet** építettek a megmaradó (még mindig igen nagy) kulcstér szisztematikus átvizsgálására: **a BOMBA-t**.

Az Enigma feltörése: a brit Bletchley Park

- A lengyel módszereket továbbfejlesztve **pár hónap alatt** minden **új fejlesztésű tárcsát és kulcsközlő módszert meg tudtak fejteni.**
- Ez azt jelenti, hogy **feltörték a napi kapocstábla állást** és meg tudták határozni az egyes **üzenetek egyedi kulcsát.**
- A leghosszabb szünet **1942. februártól októberig** tartott, amíg egy aktuális kódtábla csomagot szereztek egy **süllyedő U-559-ről.**
- Kifinomult *statisztikai és nyelvészeti módszerekkel* a **jobb oldali tárcsát** meg tudták határozni.
- A lengyel BOMBA-t többszörösen továbbfejlesztve **elektromechanikus számítógépeket** építettek: **Turing Bomb, US Navy Bomb**
- A brit haderővel együttműködve **ismert tartalmú német üzeneteket** tudtak generálni.
- Számos egyéb kriptorendszert is analizáltak: *Lorenz*, szovjet, japán, stb.

Az Enigma feltörése: a brit Bletchley Park

- A lengyel módszereket továbbfejlesztve **pár hónap alatt** minden **új fejlesztésű tárcsát és kulcsközlő módszert meg tudtak fejteni.**
- Ez azt jelenti, hogy **feltörték a napi kapocstábla állást** és meg tudták határozni az egyes **üzenetek egyedi kulcsát.**
- A leghosszabb szünet **1942. februártól októberig** tartott, amíg egy aktuális kódtábla csomagot szereztek egy **süllyedő U-559-ről.**
- Kifinomult *statisztikai és nyelvészeti módszerekkel* a **jobb oldali tárcsát** meg tudták határozni.
- A lengyel BOMBA-t többszörösen továbbfejlesztve **elektromechanikus számítógépeket** építettek: **Turing Bomb, US Navy Bomb**
- A brit haderővel együttműködve **ismert tartalmú német üzeneteket** tudtak generálni.
- Számos egyéb kriptorendszert is analizáltak: *Lorenz, szovjet, japán, stb.*

Az Enigma feltörése: a brit Bletchley Park

- A lengyel módszereket továbbfejlesztve **pár hónap alatt** minden **új fejlesztésű tárcsát és kulcsközlő módszert meg tudtak fejteni.**
- Ez azt jelenti, hogy **feltörték a napi kapocstábla állást** és meg tudták határozni az egyes **üzenetek egyedi kulcsát.**
- A leghosszabb szünet **1942. februártól októberig** tartott, amíg egy aktuális kódtábla csomagot szereztek egy **süllyedő U-559-ről.**
- Kifinomult *statisztikai és nyelvészeti módszerekkel* a **jobb oldali tárcsát** meg tudták határozni.
- A lengyel BOMBA-t többszörösen továbbfejlesztve **elektromechanikus számítógépeket** építettek: **Turing Bomb, US Navy Bomb**
- A brit haderővel együttműködve **ismert tartalmú német üzeneteket** tudtak generálni.
- Számos egyéb kriptorendszert is analizáltak: *Lorenz, szovjet, japán, stb.*

Az Enigma feltörése: a brit Bletchley Park

- A lengyel módszereket továbbfejlesztve **pár hónap alatt** minden **új fejlesztésű tárcsát és kulcsközlő módszert meg tudtak fejteni.**
- Ez azt jelenti, hogy **feltörték a napi kapocstábla állást** és meg tudták határozni az egyes **üzenetek egyedi kulcsát.**
- A leghosszabb szünet **1942. februártól októberig** tartott, amíg egy aktuális kódtábla csomagot szereztek egy **süllyedő U-559-ről.**
- Kifinomult *statisztikai és nyelvészeti módszerekkel* a **jobb oldali tárcsát** meg tudták határozni.
- A lengyel BOMBA-t többszörösen továbbfejlesztve **elektromechanikus számítógépeket** építettek: Turing Bomb, US Navy Bomb
- A brit haderővel együttműködve **ismert tartalmú német üzeneteket** tudtak generálni.
- Számos egyéb kriptorendszert is analizáltak: *Lorenz*, szovjet, japán, stb.

Az Enigma feltörése: a brit Bletchley Park

- A lengyel módszereket továbbfejlesztve **pár hónap alatt** minden **új fejlesztésű tárcsát és kulcsközlő módszert meg tudtak fejteni.**
- Ez azt jelenti, hogy **feltörték a napi kapocstábla állást** és meg tudták határozni az egyes **üzenetek egyedi kulcsát.**
- A leghosszabb szünet **1942. februártól októberig** tartott, amíg egy aktuális kódtábla csomagot szereztek egy **süllyedő U-559-ről.**
- Kifinomult *statisztikai és nyelvészeti módszerekkel* a **jobb oldali tárcsát** meg tudták határozni.
- A lengyel BOMBA-t többszörösen továbbfejlesztve **elektromechanikus számítógépeket** építettek: **Turing Bomb, US Navy Bomb**
- A brit haderővel együttműködve **ismert tartalmú német üzeneteket** tudtak generálni.
- Számos egyéb kriptorendszert is analizáltak: *Lorenz, szovjet, japán, stb.*

Az Enigma feltörése: a brit Bletchley Park

- A lengyel módszereket továbbfejlesztve **pár hónap alatt** minden **új fejlesztésű tárcsát és kulcsközlő módszert meg tudtak fejteni.**
- Ez azt jelenti, hogy **feltörték a napi kapocstábla állást** és meg tudták határozni az egyes **üzenetek egyedi kulcsát.**
- A leghosszabb szünet **1942. februártól októberig** tartott, amíg egy aktuális kódtábla csomagot szereztek egy **süllyedő U-559-ről.**
- Kifinomult *statisztikai és nyelvészeti módszerekkel* a **jobb oldali tárcsát** meg tudták határozni.
- A lengyel BOMBA-t többszörösen továbbfejlesztve **elektromechanikus számítógépeket** építettek: **Turing Bomb, US Navy Bomb**
- A brit haderővel együttműködve **ismert tartalmú német üzeneteket** tudtak generálni.
- Számos egyéb kriptorendszert is analizáltak: *Lorenz, szovjet, japán, stb.*

Az Enigma feltörése: a brit Bletchley Park

- A lengyel módszereket továbbfejlesztve **pár hónap alatt** minden **új fejlesztésű tárcsát és kulcsközlő módszert meg tudtak fejteni.**
- Ez azt jelenti, hogy **feltörték a napi kapocstábla állást** és meg tudták határozni az egyes **üzenetek egyedi kulcsát.**
- A leghosszabb szünet **1942. februártól októberig** tartott, amíg egy aktuális kódtábla csomagot szereztek egy **süllyedő U-559-ről.**
- Kifinomult *statisztikai és nyelvészeti módszerekkel* a **jobb oldali tárcsát** meg tudták határozni.
- A lengyel BOMBA-t többszörösen továbbfejlesztve **elektromechanikus számítógépeket** építettek: **Turing Bomb, US Navy Bomb**
- A brit haderővel együttműködve **ismert tartalmú német üzeneteket** tudtak generálni.
- Számos egyéb kriptorendszert is analizáltak: *Lorenz*, szovjet, japán, stb.

Alan Turing (1912-1954)



- Az egyik legnagyobb **20. századi matematikus zseni**
- Az 1930-as években lefektette a számítógépek elméletének matematikai alapjai (*Turing-gép*)
- A "Turing Bomb" gép megalkotója
- Az 1950-es években mesterséges intelligencia kutatásokat végzett (*Turing-teszt*)
- Homoszexualitása miatt 1952-ben elítélte az angol bíróság

Alan Turing (1912-1954)



- Az egyik legnagyobb **20. századi matematikus zseni**
- Az **1930-as** években lefektette a **számítógépek elméletének matematikai alapjai** (*Turing-gép*)
- A "Turing Bomb" gép megalkotója
- Az **1950-es** években **mesterséges intelligencia** kutatásokat végzett (*Turing-teszt*)
- **Homoszexualitása** miatt **1952-ben** elítélte az angol bíróság

Alan Turing (1912-1954)



- Az egyik legnagyobb **20. századi matematikus zseni**
- Az **1930-as** években lefektette a **számítógépek elméletének matematikai alapjai** (*Turing-gép*)
- A **"Turing Bomb"** gép megalkotója
- Az **1950-es** években **mesterséges intelligencia** kutatásokat végzett (*Turing-teszt*)
- **Homoszexualitása** miatt **1952-ben** elítélte az angol bíróság

Alan Turing (1912-1954)



- Az egyik legnagyobb **20. századi matematikus zseni**
- Az **1930-as** években lefektette a **számítógépek elméletének matematikai alapjai** (*Turing-gép*)
- A **"Turing Bomb"** gép megalkotója
- Az **1950-es** években **mesterséges intelligencia** kutatásokat végzett (*Turing-teszt*)
- **Homoszexualitása** miatt **1952-ben** elítélte az angol bíróság

Alan Turing (1912-1954)



- Az egyik legnagyobb **20. századi matematikus zseni**
- Az **1930-as** években lefektette a **számítógépek elméletének matematikai alapjai** (*Turing-gép*)
- A **"Turing Bomb"** gép megalkotója
- Az **1950-es** években **mesterséges intelligencia** kutatásokat végzett (*Turing-teszt*)
- **Homoszexualitása** miatt **1952-ben** elítélte az angol bíróság

Table of Contents

- 1 A titkosítások elméleti alapelvei
- 2 Az Enigma-rendszerek működése
- 3 Az Enigma sebezhetőségei
- 4 Napjaink kriptorendszerei**

Szimmetrikus kulcsú kriptográfia

SZIMMETRIA

Ugyanaz a kulcs szolgál rejtjelezésre és visszafejtésre.

- 1976: **DES** (Data Encryption Standard)
- 2001: **AES** (Advanced Encryption Standard)
- AES demó: <http://www.formaestudio.com/rijndaelinspector/>
- **Előny:** Gyorsaság, kicsi memóriaigény, matematikai módszerekkel jól ellenőrizhető biztonság („keverési” tulajdonságok)
- **Hátrány:** A kommunikáló feleknek előre meg kell állapodni a **közös titkos kulcsban** (*key management*)

Szimmetrikus kulcsú kriptográfia

SZIMMETRIA

Ugyanaz a kulcs szolgál rejtjelezésre és visszafejtésre.

- 1976: **DES** (Data Encryption Standard)
- 2001: **AES** (Advanced Encryption Standard)
- AES demó: <http://www.formaestudio.com/rijndaelinspector/>
- **Előny:** Gyorsaság, kicsi memóriaigény, matematikai módszerekkel jól ellenőrizhető biztonság („keverési” tulajdonságok)
- **Hátrány:** A kommunikáló feleknek előre meg kell állapodni a **közös titkos kulcsban** (*key management*)

Szimmetrikus kulcsú kriptográfia

SZIMMETRIA

Ugyanaz a kulcs szolgál rejtjelezésre és visszafejtésre.

- 1976: **DES** (Data Encryption Standard)
- 2001: **AES** (Advanced Encryption Standard)
- AES demó: <http://www.formaestudio.com/rijndaelinspector/>
- **Előny:** Gyorsaság, kicsi memóriaigény, matematikai módszerekkel jól ellenőrizhető biztonság („keverési” tulajdonságok)
- **Hátrány:** A kommunikáló feleknek előre meg kell állapodni a **közös titkos kulcsban** (*key management*)

Szimmetrikus kulcsú kriptográfia

SZIMMETRIA

Ugyanaz a kulcs szolgál rejtjelezésre és visszafejtésre.

- 1976: **DES** (Data Encryption Standard)
- 2001: **AES** (Advanced Encryption Standard)
- AES demó: <http://www.formaestudio.com/rijndaelinspector/>
- **Előny:** Gyorsaság, kicsi memóriaigény, matematikai módszerekkel jól ellenőrizhető biztonság („keverési” tulajdonságok)
- **Hátrány:** A kommunikáló feleknek előre meg kell állapodni a **közös titkos kulcsban** (*key management*)

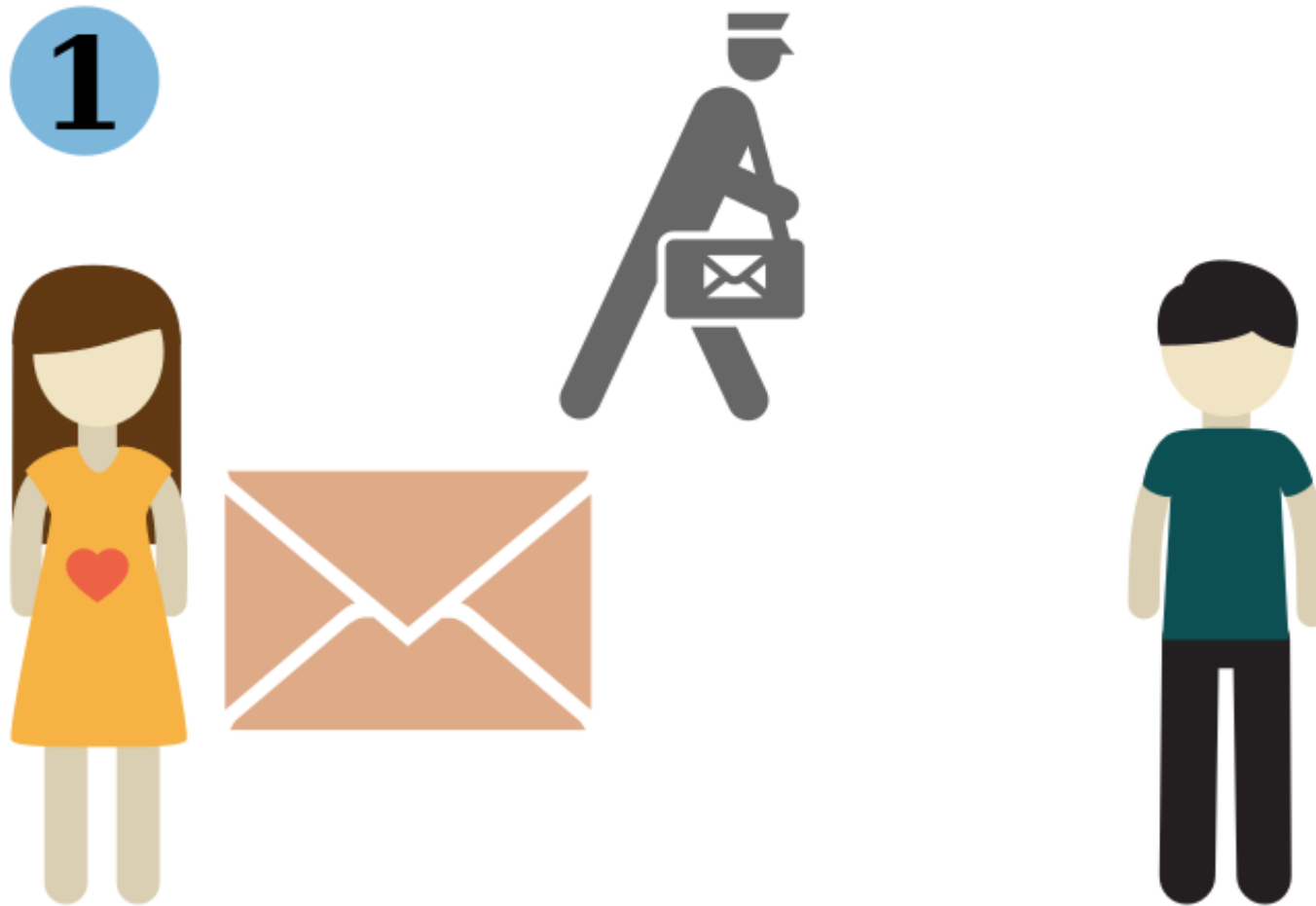
Szimmetrikus kulcsú kriptográfia

SZIMMETRIA

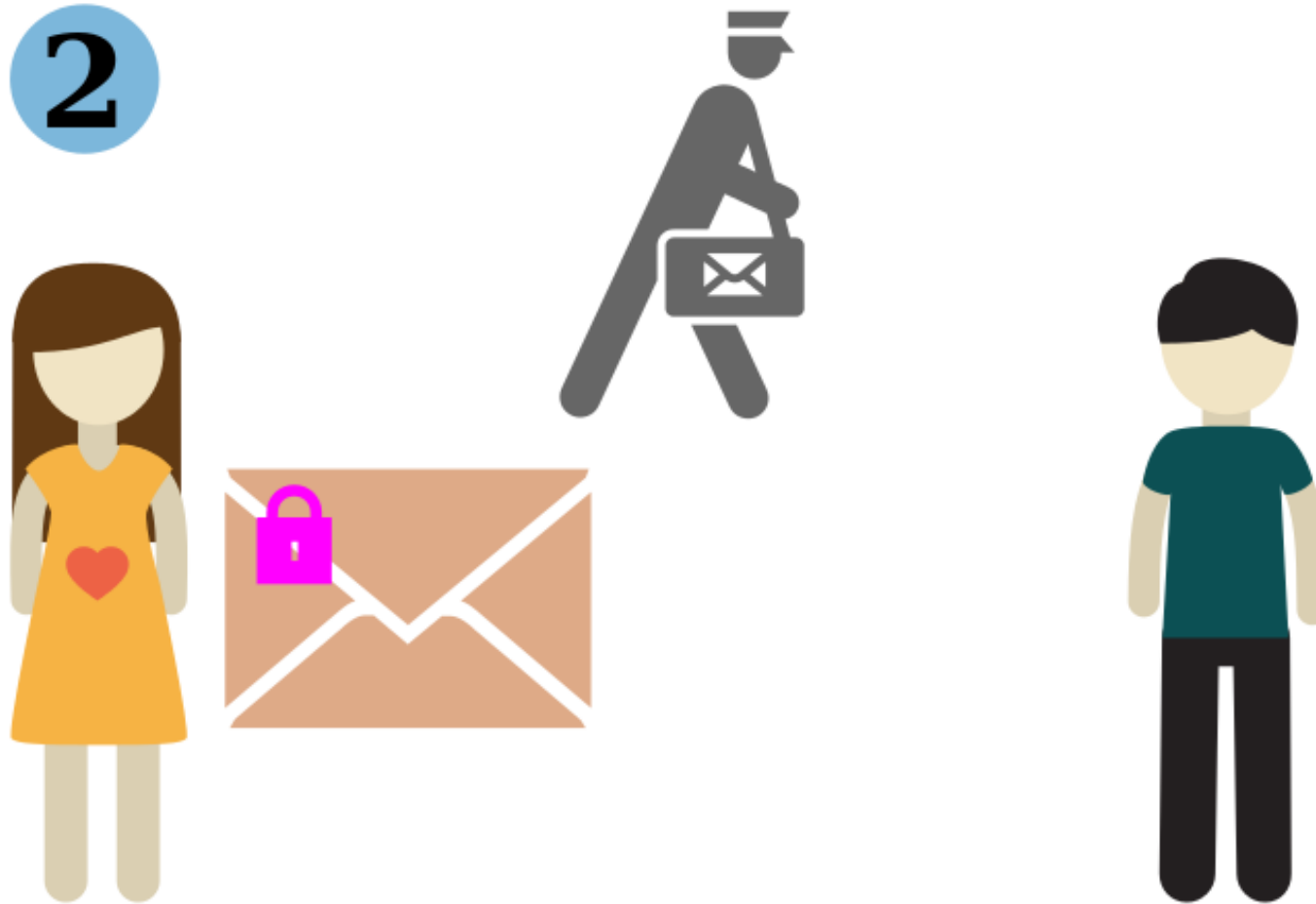
Ugyanaz a kulcs szolgál rejtjelezésre és visszafejtésre.

- 1976: **DES** (Data Encryption Standard)
- 2001: **AES** (Advanced Encryption Standard)
- AES demó: <http://www.formaestudio.com/rijndaelinspector/>
- **Előny:** Gyorsaság, kicsi memóriaigény, matematikai módszerekkel jól ellenőrizhető biztonság („keverési” tulajdonságok)
- **Hátrány:** A kommunikáló feleknek előre meg kell állapodni a **közös titkos kulcsban** (*key management*)

Kulcsmenedzsment: A Diffie-Hellman–kulcscsere (1976)



Kulcsmenedzsment: A Diffie-Hellman–kulcscsere (1976)



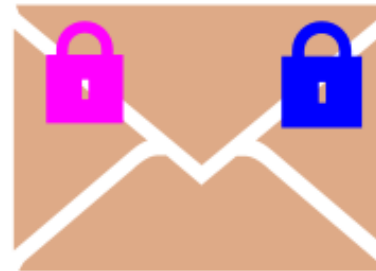
Kulcsmenedzsment: A Diffie-Hellman–kulcscsere (1976)

3

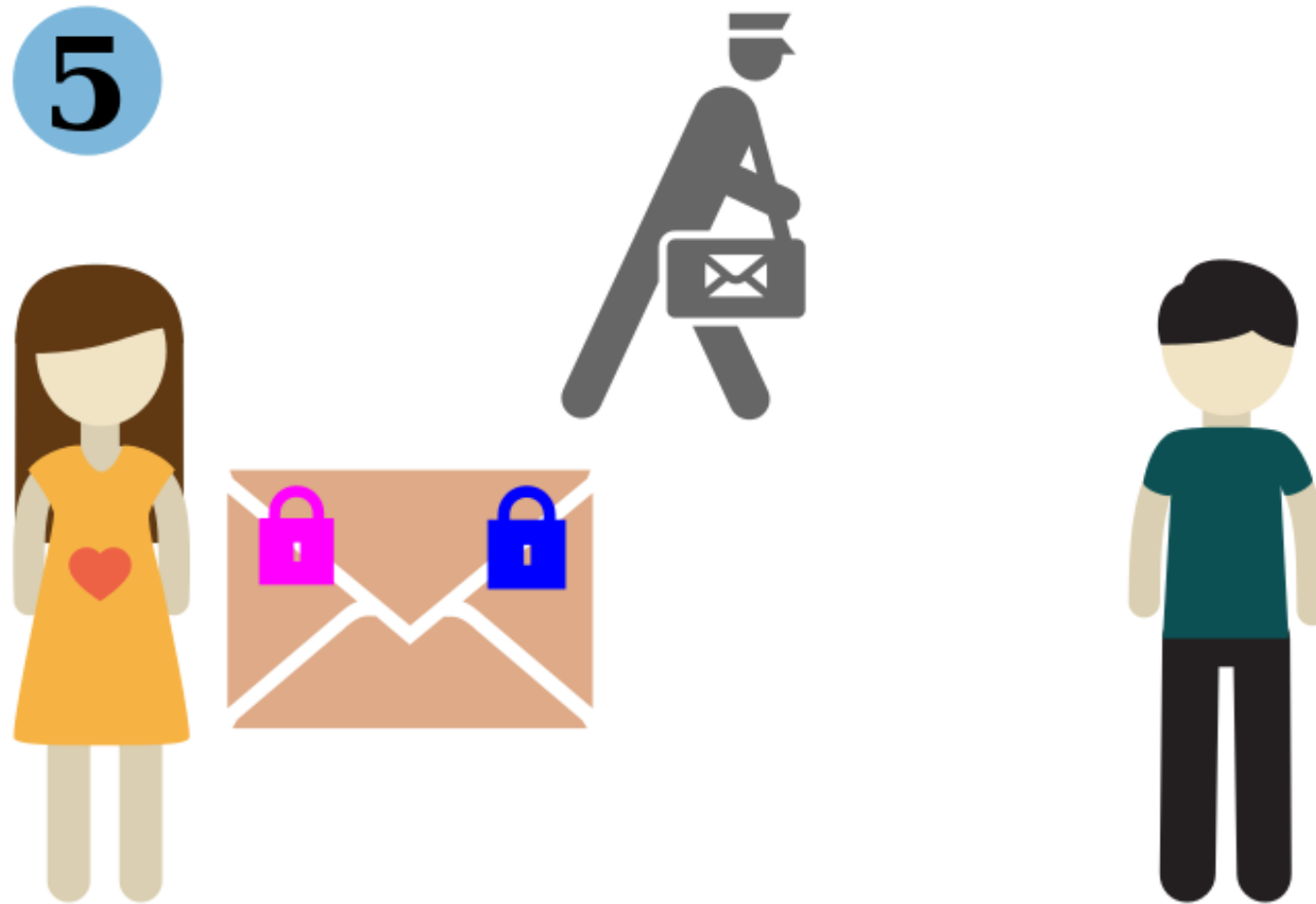


Kulcsmenedzsment: A Diffie-Hellman–kulcscsere (1976)

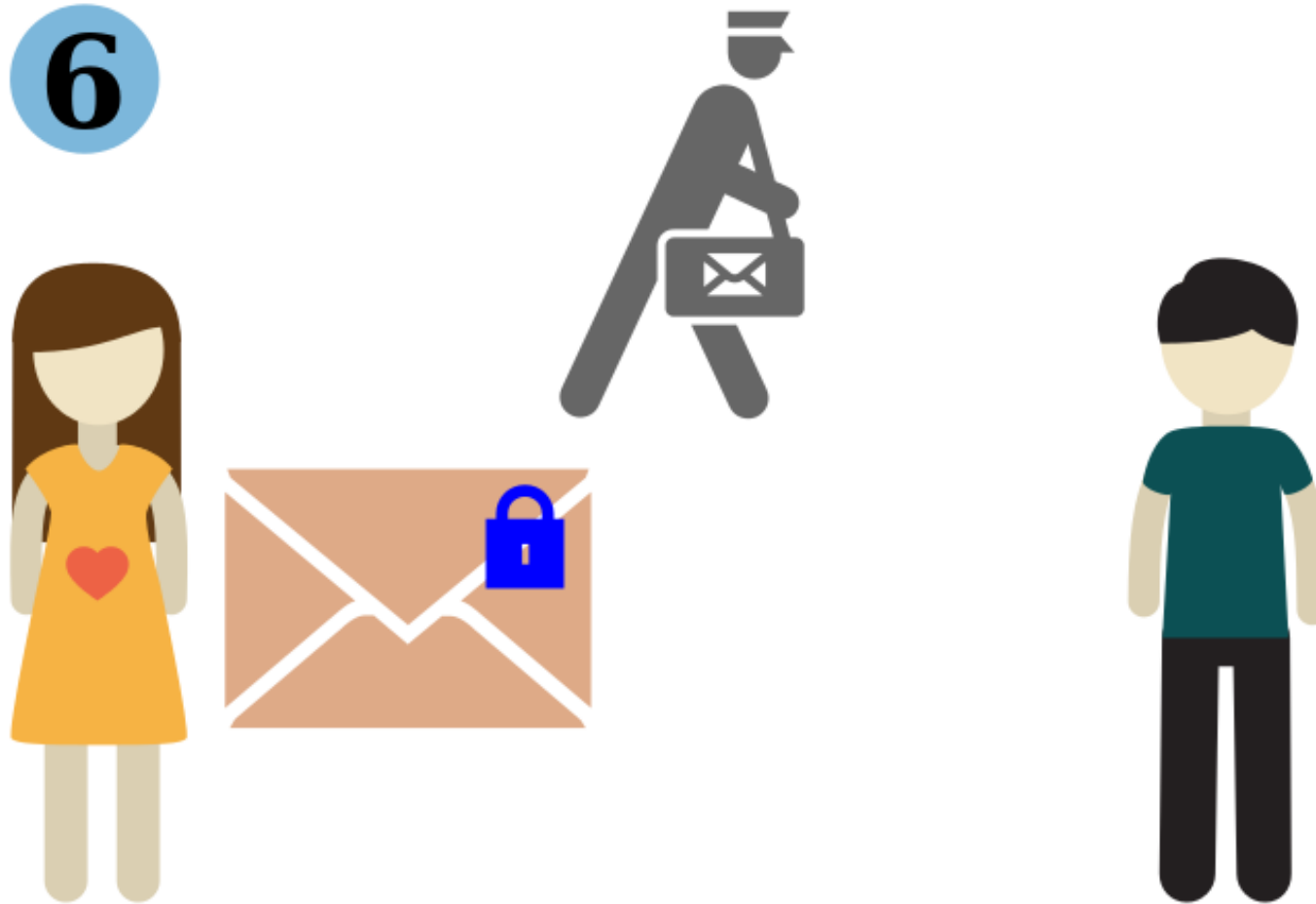
4



Kulcsmenedzsment: A Diffie-Hellman–kulcscsere (1976)



Kulcsmenedzsment: A Diffie-Hellman–kulcscsere (1976)



Kulcsmenedzsment: A Diffie-Hellman–kulcscsere (1976)

7



Kulcsmenedzsment: A Diffie-Hellman–kulcscsere (1976)

8



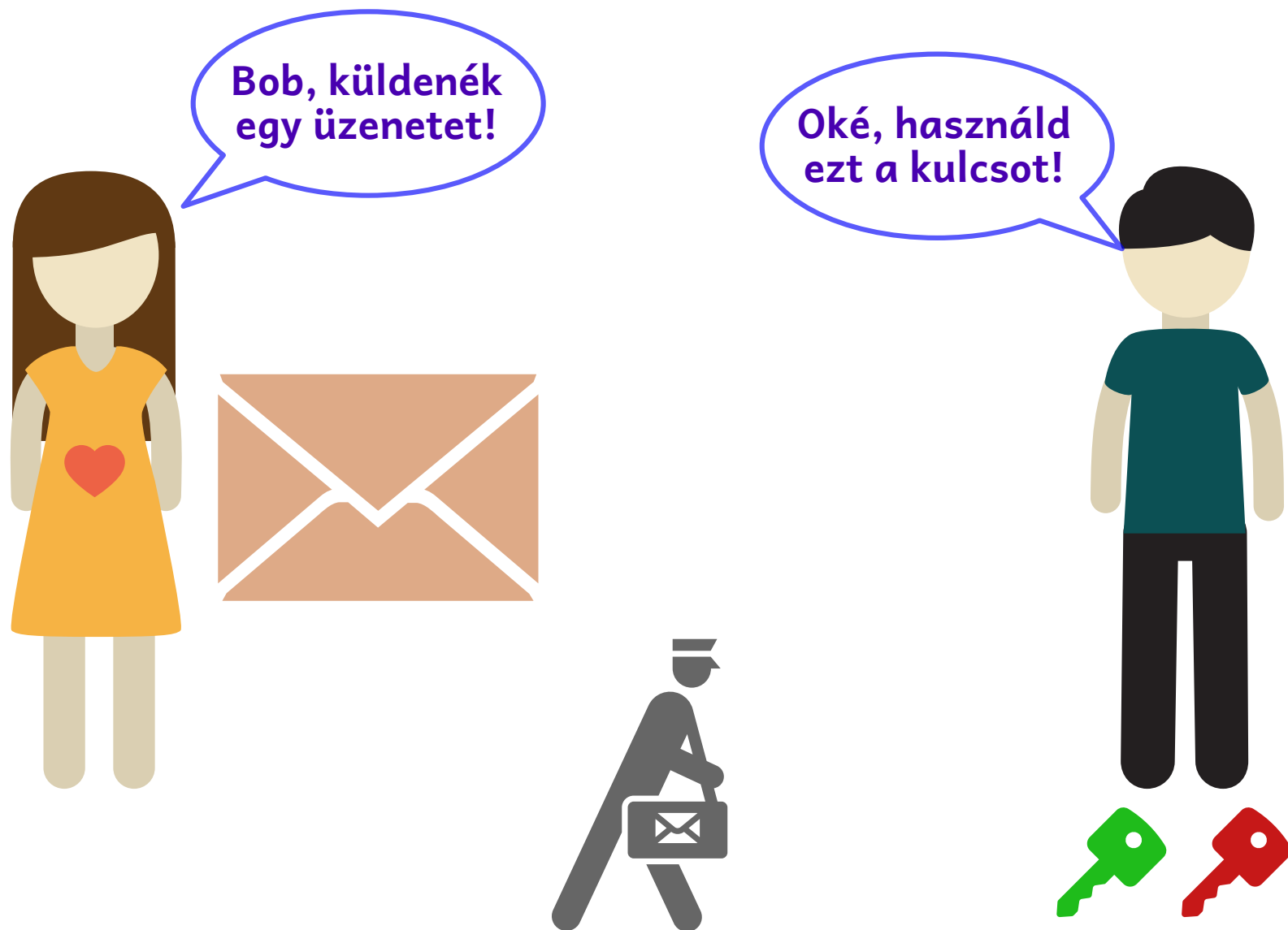
Nyilvános (aszimmetrikus) kulcsú kriptográfia

ASSZIMETRIA

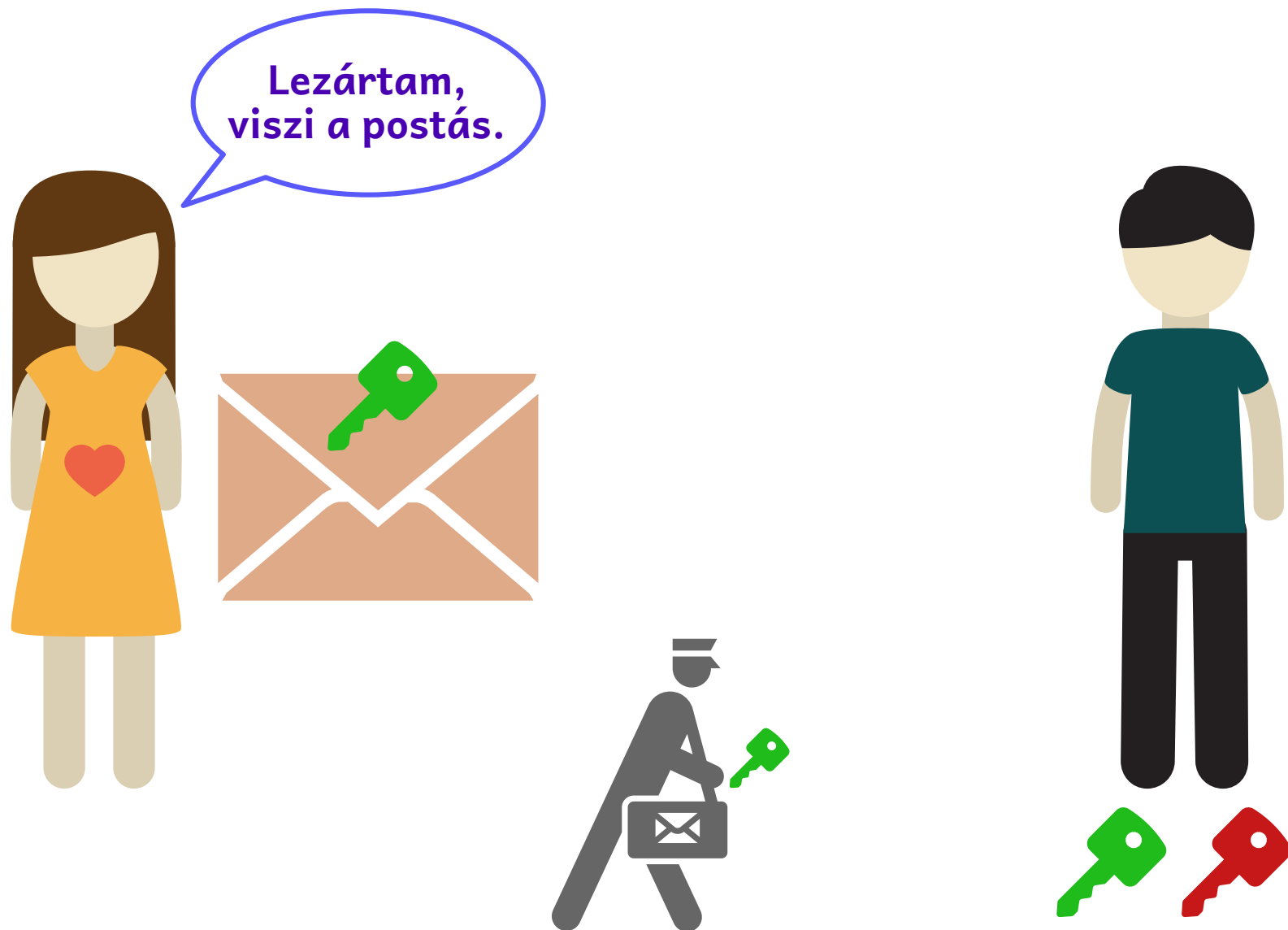
Két **különböző kulcsot** használunk a rejtjelezésre illetve a visszafejtésre: egy nyilvános és egy **privát** kulcsot

- Alice nyílt szövege Bobnak + Bob nyilvános kulcsa = rejtjelezett szöveg Bobnak
- rejtjelezett szöveg Bobnak + Bob privát kulcsa = Alice nyílt szövege Bobnak

Nyilvános (aszimmetrikus) kulcsú kriptográfia



Nyilvános (aszimmetrikus) kulcsú kriptográfia



Nyilvános (aszimmetrikus) kulcsú kriptográfia



Nyilvános (aszimmetrikus) kulcsú kriptográfia

ASSZIMETRIA

Két **különböző kulcsot** használunk a rejtjelezésre illetve a visszafejtésre: egy **nyilvános** és egy **privát** kulcsot

- A nyilvános kulcsból a privát kulcs kiszámítása **elméletben lehetséges**, de a **gyakorlatban nem**
- 1978: **RSA** (RONALD RIVEST, ADI SHAMIR és LEN ADLEMAN)
- Az RSA biztonsága azon múlik, hogy tudunk-e **több száz számjegyből** álló számokat **prímtényezőkre** bontani.
- Pontosabban, adott a, k, n egészek esetén

$$x^k = a \pmod{n}$$

akkor oldható meg hatékonyan, ha ismerjük n prímtényezőös felbontását.

- Hagyományos komputerrel ez **nem megy**, de.....

Nyilvános (aszimmetrikus) kulcsú kriptográfia

ASSZIMETRIA

Két **különböző kulcsot** használunk a rejtjelezésre illetve a visszafejtésre: egy **nyilvános** és egy **privát** kulcsot

- A nyilvános kulcsból a privát kulcs kiszámítása **elméletben lehetséges**, de a **gyakorlatban nem**
- 1978: **RSA** (RONALD RIVEST, ADI SHAMIR és LEN ADLEMAN)
- Az RSA biztonsága azon múlik, hogy tudunk-e **több száz számjegyből** álló számokat **prímtényezőkre** bontani.
- Pontosabban, adott a, k, n egészek esetén

$$x^k = a \pmod{n}$$

akkor oldható meg hatékonyan, ha ismerjük n prímtényezős felbontását.

- Hagyományos komputerrel ez **nem megy**, de.....

Nyilvános (aszimmetrikus) kulcsú kriptográfia

ASSZIMETRIA

Két **különböző kulcsot** használunk a rejtjelezésre illetve a visszafejtésre: egy **nyilvános** és egy **privát** kulcsot

- A nyilvános kulcsból a privát kulcs kiszámítása **elméletben lehetséges**, de a **gyakorlatban nem**
- 1978: **RSA** (RONALD RIVEST, ADI SHAMIR és LEN ADLEMAN)
- Az RSA biztonsága azon múlik, hogy tudunk-e **több száz számjegyből** álló számokat **prímtényezőkre** bontani.
- Pontosabban, adott a, k, n egészek esetén

$$x^k = a \pmod{n}$$

akkor oldható meg hatékonyan, ha ismerjük n prímtényezős felbontását.

- Hagyományos komputerrel ez **nem megy**, de.....

Nyilvános (aszimmetrikus) kulcsú kriptográfia

ASSZIMETRIA

Két **különböző kulcsot** használunk a rejtjelezésre illetve a visszafejtésre: egy **nyilvános** és egy **privát** kulcsot

- A nyilvános kulcsból a privát kulcs kiszámítása **elméletben lehetséges**, de a **gyakorlatban nem**
- 1978: **RSA** (RONALD RIVEST, ADI SHAMIR és LEN ADLEMAN)
- Az RSA biztonsága azon múlik, hogy tudunk-e **több száz számjegyből** álló számokat **prímtényezőkre** bontani.
- **Pontosabban**, adott a, k, n egészek esetén

$$x^k = a \pmod{n}$$

akkor oldható meg hatékonyan, ha ismerjük n prímtényezőös felbontását.

- Hagyományos komputerrel ez **nem megy**, de.....

Nyilvános (aszimmetrikus) kulcsú kriptográfia

ASSZIMETRIA

Két **különböző kulcsot** használunk a rejtjelezésre illetve a visszafejtésre: egy **nyilvános** és egy **privát** kulcsot

- A nyilvános kulcsból a privát kulcs kiszámítása **elméletben lehetséges**, de a **gyakorlatban nem**
- 1978: **RSA** (RONALD RIVEST, ADI SHAMIR és LEN ADLEMAN)
- Az RSA biztonsága azon múlik, hogy tudunk-e **több száz számjegyből** álló számokat **prímtényezőkre** bontani.
- **Pontosabban**, adott a, k, n egészek esetén

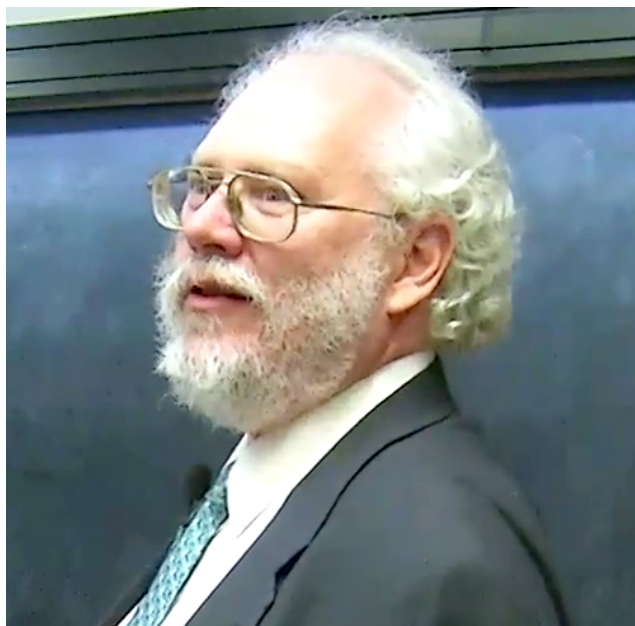
$$x^k = a \pmod{n}$$

akkor oldható meg hatékonyan, ha ismerjük n prímtényezőös felbontását.

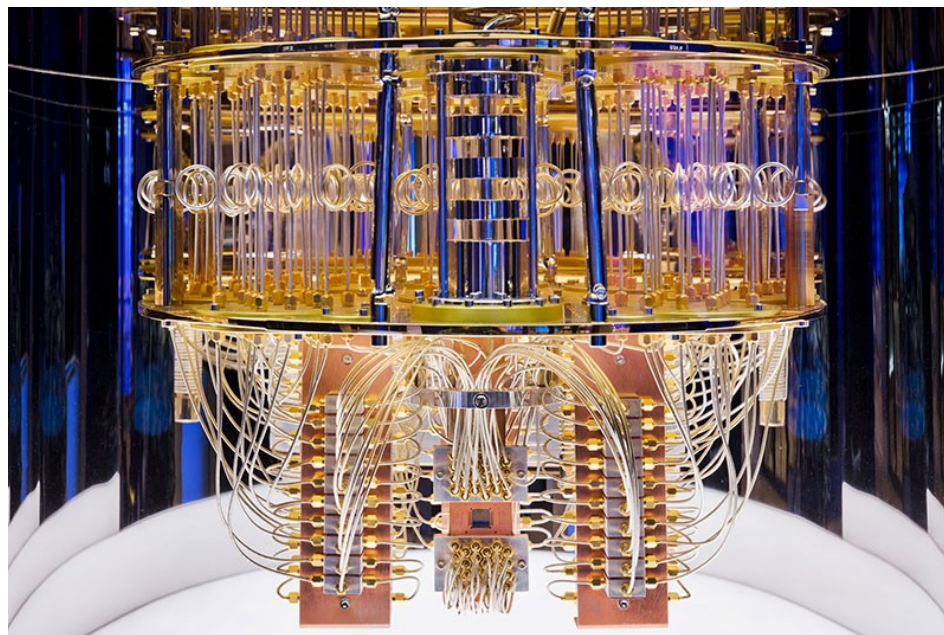
- Hagyományos komputerrel ez **nem megy, de.....**

A kvantumszámítógépes támadás

- A jelenleg használt nyilvános kulcsú titkosítások védtelenek a **KVANTUMSZÁMÍTÓGÉPES TÁMADÁSSAL** szemben
- **Peter Shor** 1994-es faktorizációs kvantumalgoritmus + sok modern fejlemény



Peter Shor (MIT) in 2017



IBM 100-qubit quantum computer in 2021

Recent buzzwords

- Hibrid rendszerek
- Digitális aláírás, hitelesítés (*authentication*)
- Titokmegosztó (*secret sharing*) rendszerek
- Kriptovaluták
- Oldalcsatornás támadások
- Álvéletlen (*pseudorandom*) sorozatok
- Poszt-kvantum kriptográfia (**NIST PQC Challenge**)

Recent buzzwords

- Hibrid rendszerek
- Digitális aláírás, hitelesítés (*authentication*)
- Titokmegosztó (*secret sharing*) rendszerek
- Kriptovaluták
- Oldalcsatornás támadások
- Álvéletlen (*pseudorandom*) sorozatok
- Poszt-kvantum kriptográfia (**NIST PQC Challenge**)

Recent buzzwords

- Hibrid rendszerek
- Digitális aláírás, hitelesítés (*authentication*)
- Titokmegosztó (*secret sharing*) rendszerek
- Kriptovaluták
- Oldalcsatornás támadások
- Álvéletlen (*pseudorandom*) sorozatok
- Poszt-kvantum kriptográfia (**NIST PQC Challenge**)

Recent buzzwords

- Hibrid rendszerek
- Digitális aláírás, hitelesítés (*authentication*)
- Titokmegosztó (*secret sharing*) rendszerek
- Kriptovaluták
- Oldalcsatornás támadások
- Álvéletlen (*pseudorandom*) sorozatok
- Poszt-kvantum kriptográfia (**NIST PQC Challenge**)

Recent buzzwords

- Hibrid rendszerek
- Digitális aláírás, hitelesítés (*authentication*)
- Titokmegosztó (*secret sharing*) rendszerek
- Kriptovaluták
- Oldalcsatornás támadások
- Álvéletlen (*pseudorandom*) sorozatok
- Poszt-kvantum kriptográfia (**NIST PQC Challenge**)

Recent buzzwords

- Hibrid rendszerek
- Digitális aláírás, hitelesítés (*authentication*)
- Titokmegosztó (*secret sharing*) rendszerek
- Kriptovaluták
- Oldalcsatornás támadások
- Álvéletlen (*pseudorandom*) sorozatok
- Poszt-kvantum kriptográfia (**NIST PQC Challenge**)

Recent buzzwords

- Hibrid rendszerek
- Digitális aláírás, hitelesítés (*authentication*)
- Titokmegosztó (*secret sharing*) rendszerek
- Kriptovaluták
- Oldalcsatornás támadások
- Álvéletlen (*pseudorandom*) sorozatok
- Poszt-kvantum kriptográfia (**NIST PQC Challenge**)