Titkosítási matematika

BME TTK Matematika Szakkör

2026. október 26.



Kriptográfia

- Görögből: kryptós = „rejtett”, gráphein = „írni”
- Egy kommunikációs folyamat során továbbított nyilvános üzenetet akkor nevezünk titkos(ított)nak, ha a feladó olyan formá(tum)ban küldi, amit olvasni vagy fogadni esetleg többen is tudnak, de megérteni csak a fogadók egy megcélzott csoportja.
- Példa üzenet:

$$\text{Szia Péter!}$$

- Titkos kulccsal titkosítva:

$$\textit{CJSKZODOB}$$

- Kódolva Base64-kódolással:

$$\textit{U3ppYSwgUMOpdGVyIQ} ==$$

Kriptográfia

Mitől biztonságos egy titkos üzenet?

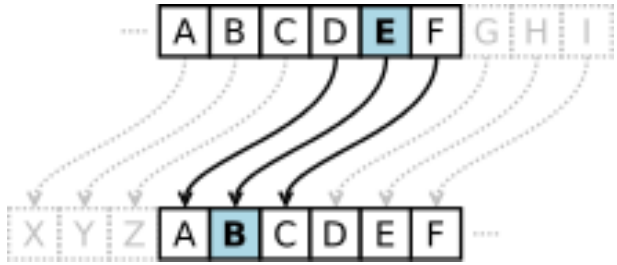
- Erős titkosítási algoritmus
- A titkos kulcs védelme
- Biztonságos kulcscsere
- Az üzenet sértetlensége és hitelessége





Rejtjelező eljárások

- Caesar chiper



Plain	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
Cipher	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

- Vigener chiper

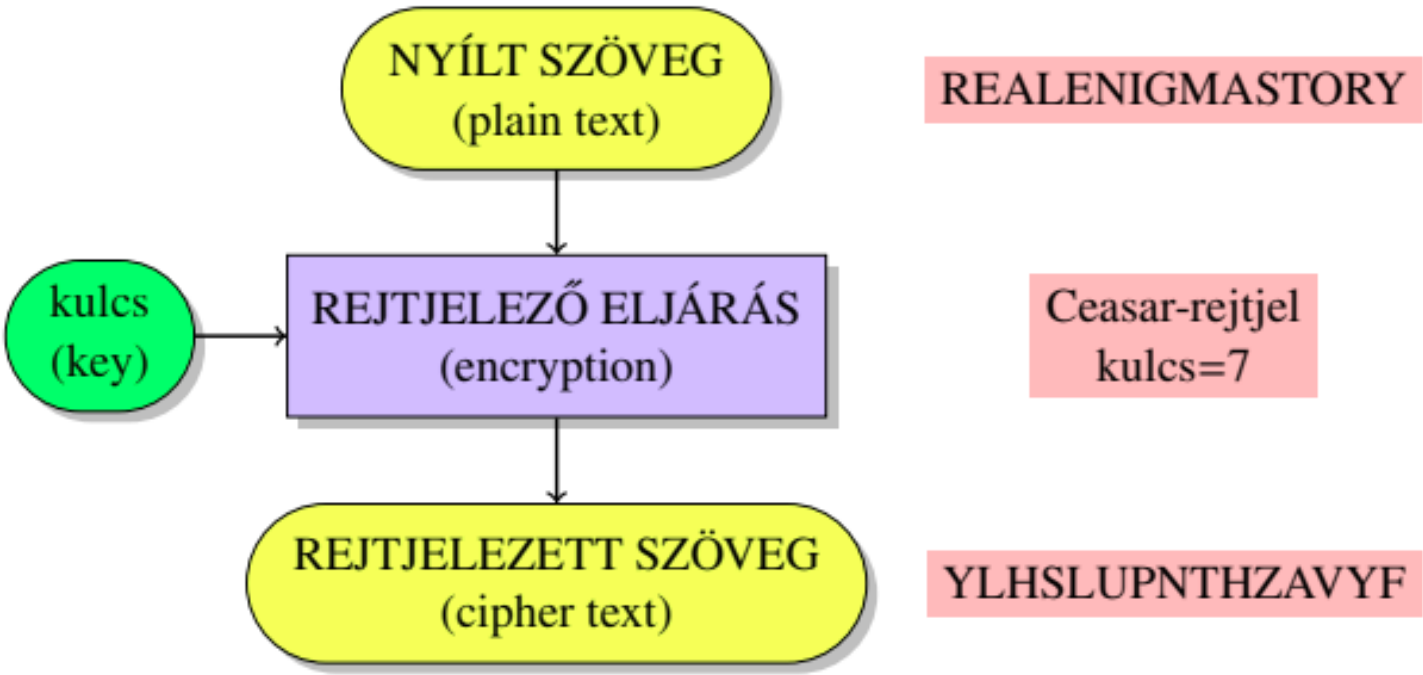
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T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

Plaintext: `attackatdawn`

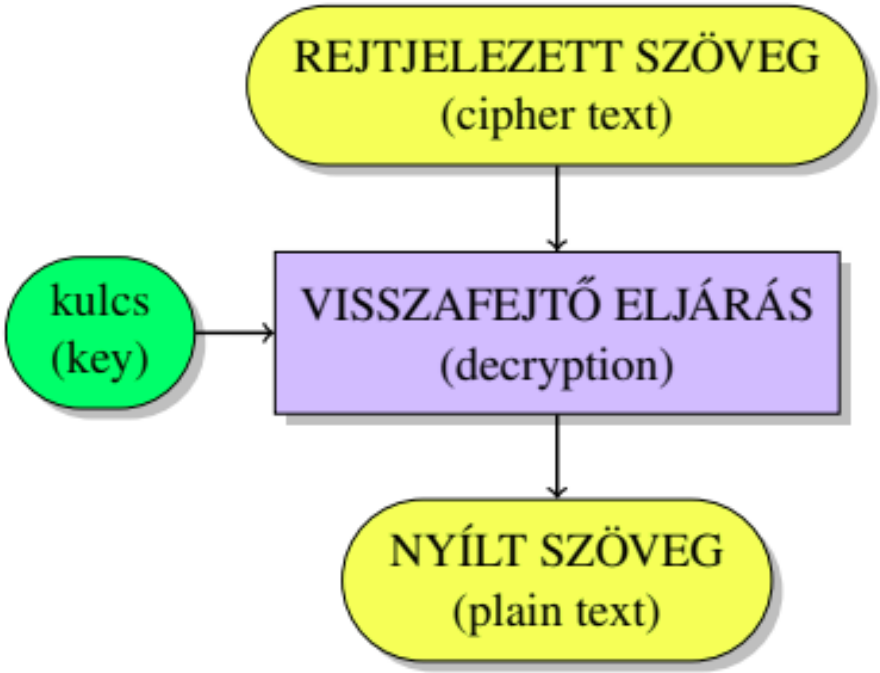
Key: `LEMONLEMONLE`

Ciphertext: `LXFOPVEFRNHR`

Rejtjelezés



Visszafejtés



GQJYHMQJDUFWP

Ceasar-rejtjel
kulcs=-5

BLETCHLEYPARK

Kód feltörése

Brute force = összes lehetőség végigpróbálása

- Ceasar-rejtjel: 26 lehetőség
- Vigenere-rejtjel: k hosszú kulcs esetén 26^k lehetőség!
  $k = 10$ esetén, ha másodpercenként 10^6 lehetőséget nézünk meg

$$\frac{26^{10}}{10^6 \cdot 60 \cdot 60 \cdot 24 \cdot 365} \approx 4.48 \text{ év}$$

Gyakoriság elemzés: többször előforduló / azonos karakterek keresése
Nyílt szöveges támadás: a támadó kiválaszt bizonyos bemeneti szövegeket, és megfigyeli, hogyan titkosítja őket a rendszer
Szótáras támadás: gyakori kulcsok, jelszavak kipróbálása
Side-channel attack: végrehajtás közben keletkező mellékes információkat vizsgálja, például a futási időt, az energiafogyasztást
Matematikai támadás: az algoritmus matematikai szerkezetét használják
Differenciális kriptoanalízis: bemenetek közötti különbségek hatását vizsgálja a titkosított kimeneteken

A Kerckhoff-féle alapelvek és a "katasztrófa forgatókönyv"

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 „katasztrófa-forgatókönyv" 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.

9/31

NSU Crypto verseny

NSUCRYPTO

Login Registration

Olympiad 2021
Results

Home
News
Participation outline
Committees & Sponsors

International Olympiad in Cryptography
Non-Stop University CRYPTO

We are inviting you to take part in

The Ninth International Olympiad in Cryptography NSUCRYPTO'2022!

Everybody can participate: **school students, university students, professionals**! It consists of two independent the Internet rounds:

- the first round (individual): **October 16, 2022;**
- the second round (team): **October 17 – 24, 2022.**

Read, what other participants write about NSUCRYPTO!
Have a look on the problems from the previous Olympiads and their solutions. Join us!



Moduláris aritmetika - műveletek maradékosztályokkal

Megjegyzés

$a \equiv b \mod n$ jelentése: a-nak az n-nel vett osztási maradéka b.
Például: $8 \equiv 2 \mod 3$, *vagy* $15 \equiv 4 \mod 11$.

- Caesar-rejtjel: a betűket számokkal helyettesítjük 1-től 26-ig:

$$A = 1, \quad B = 2, \quad \ldots \quad Z = 26.$$

- $k \in \{1, \ldots, 26\}$ a titkos kulcs
- Elkódoló függvény:

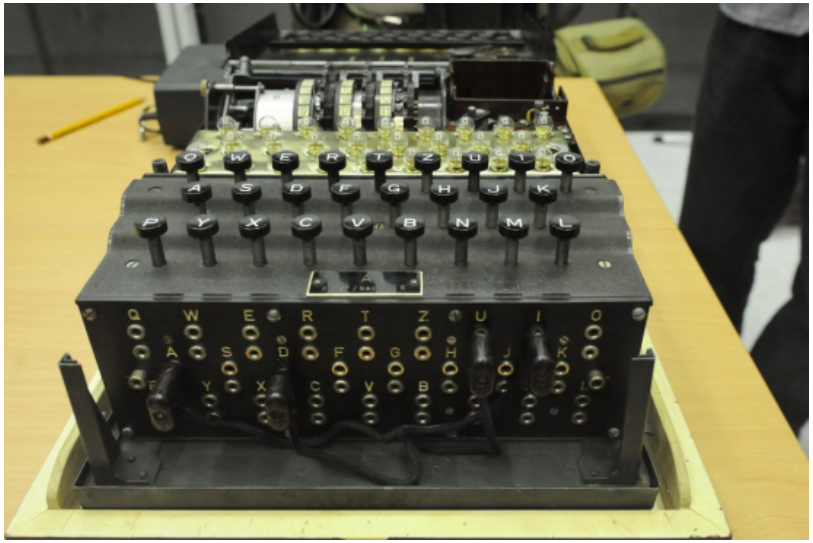
$$E_k(x) = x + k \mod 26$$

- Dekódoló függvény:

$$D_k(x) = x - k \mod 26$$

Rejtjelező eljárások - II. világháború

- Enigma



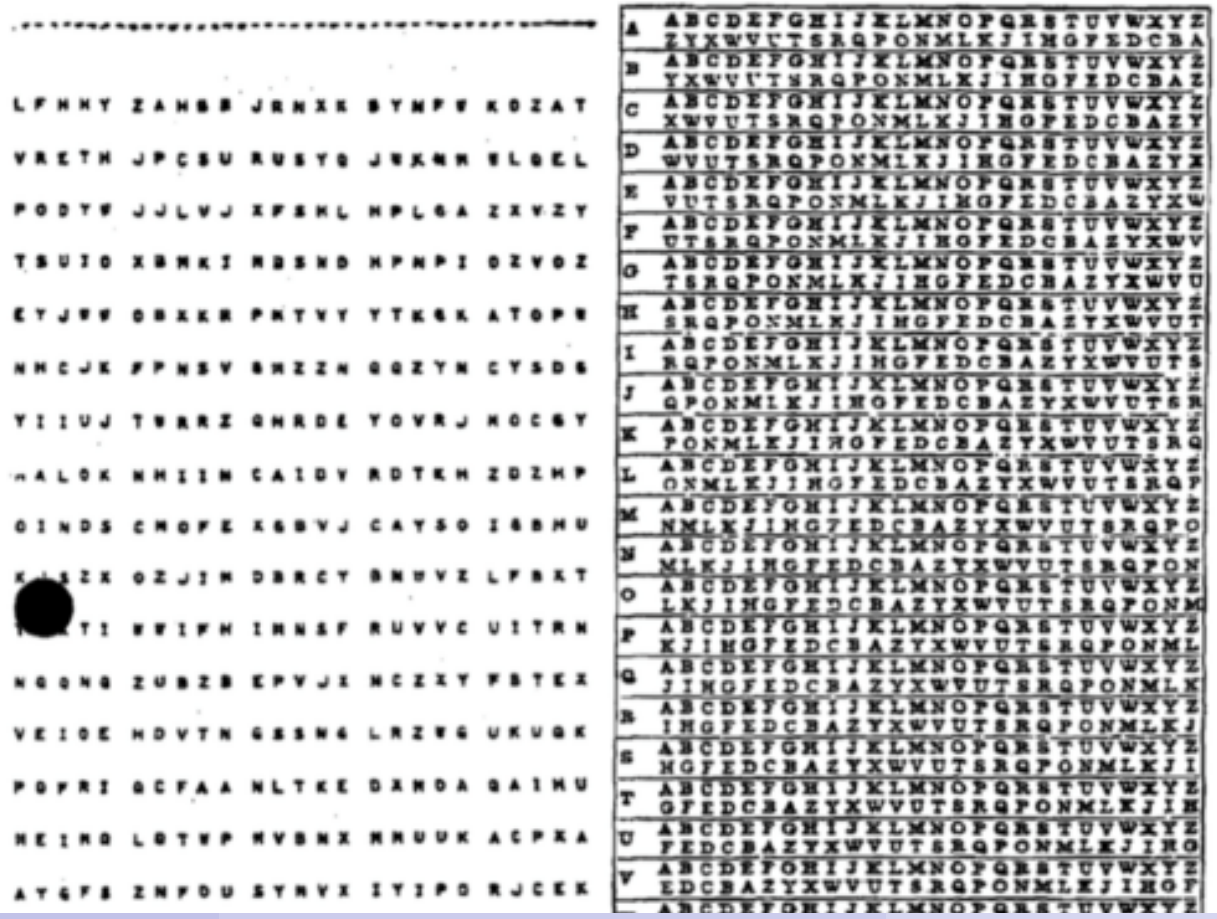
$n =$ kapcsolótábla mérete (hány átkötés történik egy leütés után).

$$\frac{1}{n!}\prod_{i=1}^{n}\frac{(26-2i+2)(26-2i+1)}{2}=\frac{26!}{2^n n!(26-2n)!}$$

Ez például $n = 10$ esetén 150 738 274 937 250 lehetőség.

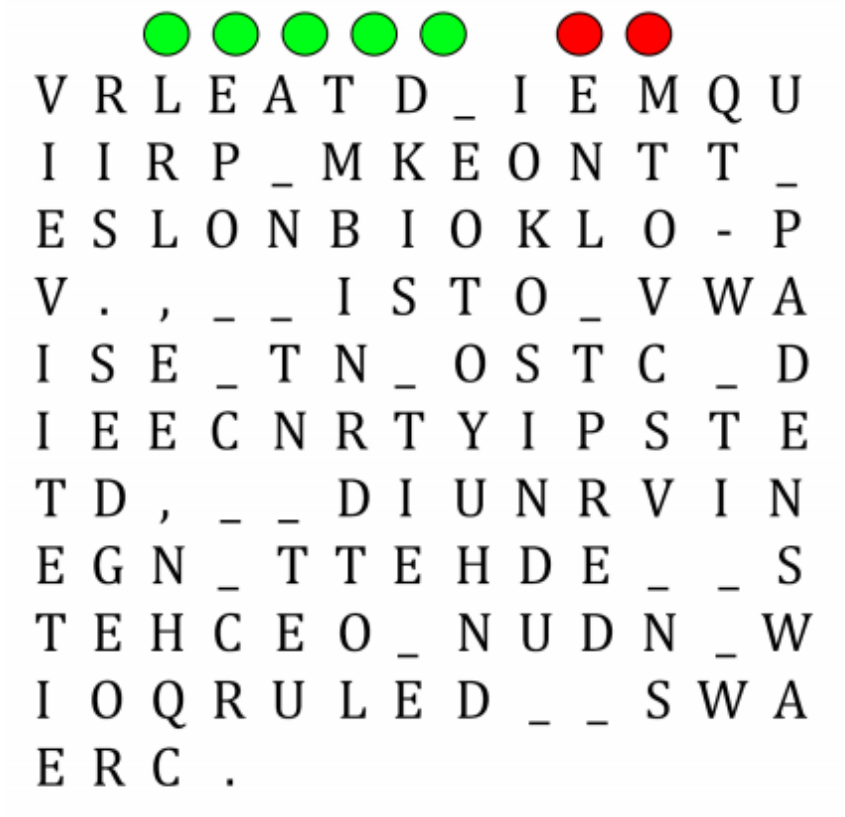
Rejtjelező eljárások - II. világháború

- Sobol - P (Vladimir Kotelnikov)
  "One-time-pad" eljárás:
  - Kulcs legalább olyan hosszú mint az üzenet
  - Kulcs titkos és egyszer használatos
  - Kulcs véletlenszerűen generált

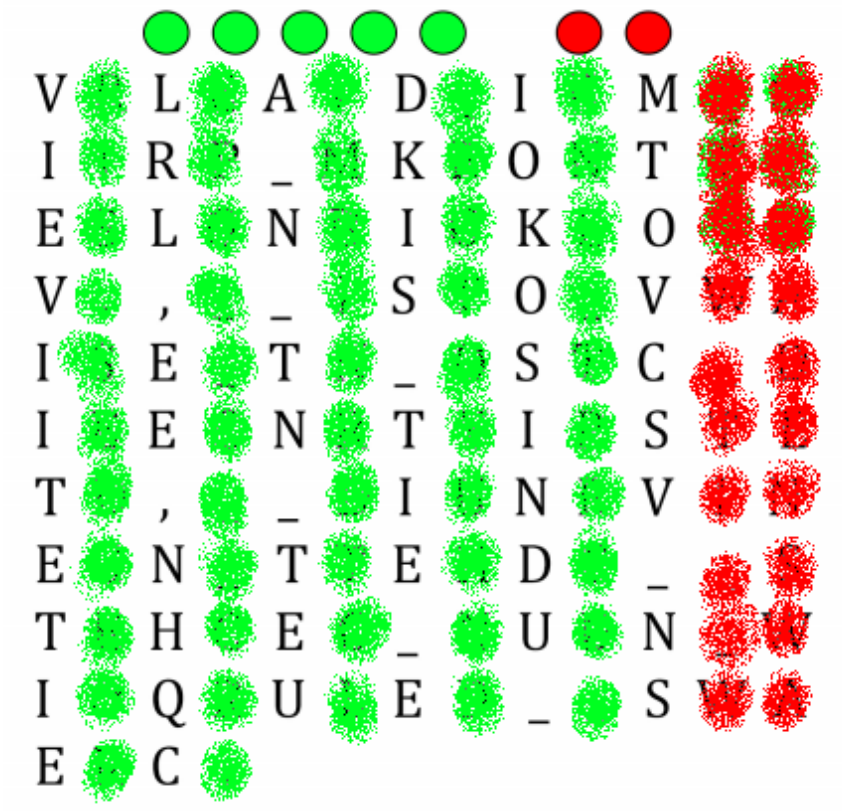


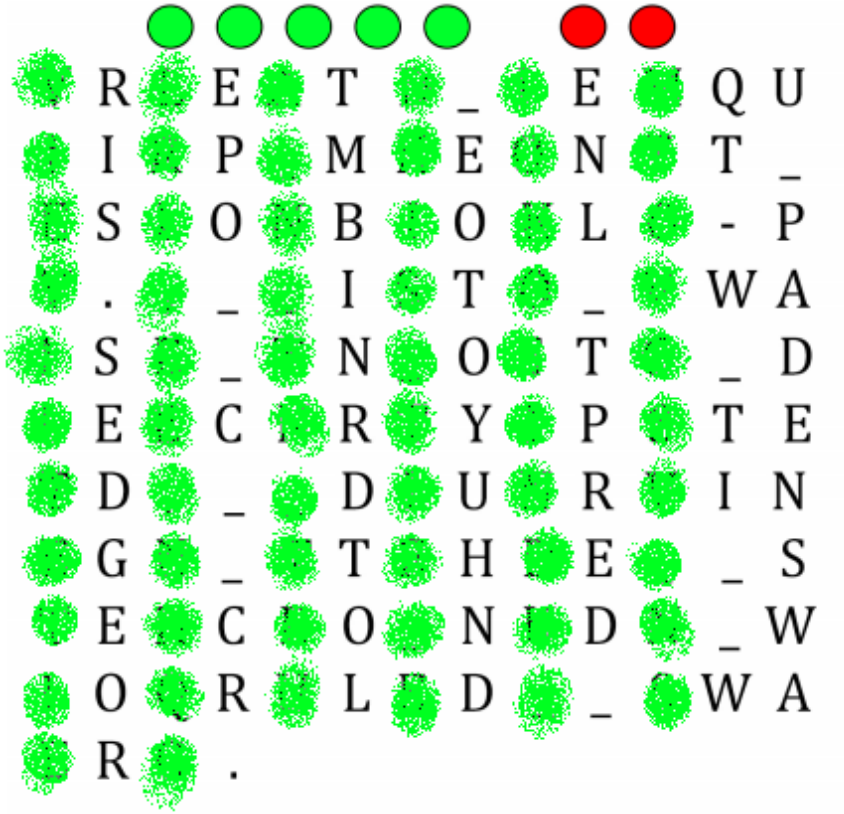
Feladat 1.

Problem 1. «Have a look and read!»



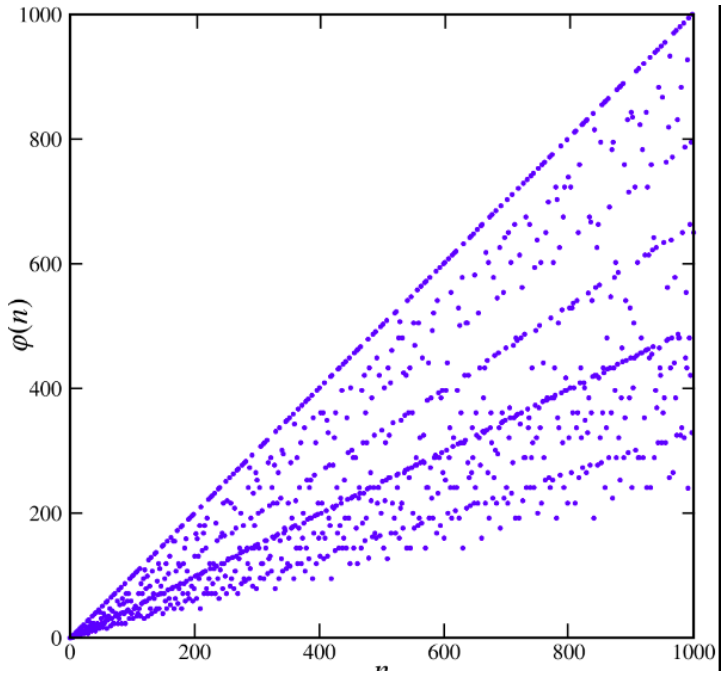
Megoldás 1.


V L A D I M
I R _ K O T
E L N I K O
V , _ S O V
I E T _ S C
I E N T I S
T , _ I N V
E N T E D _
T H E _ U N
I Q U E _ S
E C


R E T _ E Q U
I P M E N T _
S O B O L - P
. _ I T _ W A
S _ N O T _ D
E C R Y P T E
D _ D U R I N
G _ T H E _ S
E C O N D _ W
O R L D _ W A
R .

Euler-függvény

- n pozitív egész szám esetén $\varphi(n)$ jelöli az n-nél nem nagyobb, n-hez relatív prím pozitív egészek számát
- Ha p prím, akkor $\varphi(p) = p - 1$.



$$\varphi(n) = n \prod_{i=1}^{m} \left(1 - \frac{1}{p_i}\right)$$

Még egy kis számelmélet

Tétel (Kis Fermat-tétel)

Legyen p prím és $a \in \mathbb{Z}$ relatív prím a p-hez, ekkor

$$a^{p-1} \equiv 1 \mod p$$

Tétel (Euler-Fermat-tétel)

Ha a és m egymáshoz relatív prímek, akkor

$$a^{\varphi(m)} \equiv 1 \mod m$$

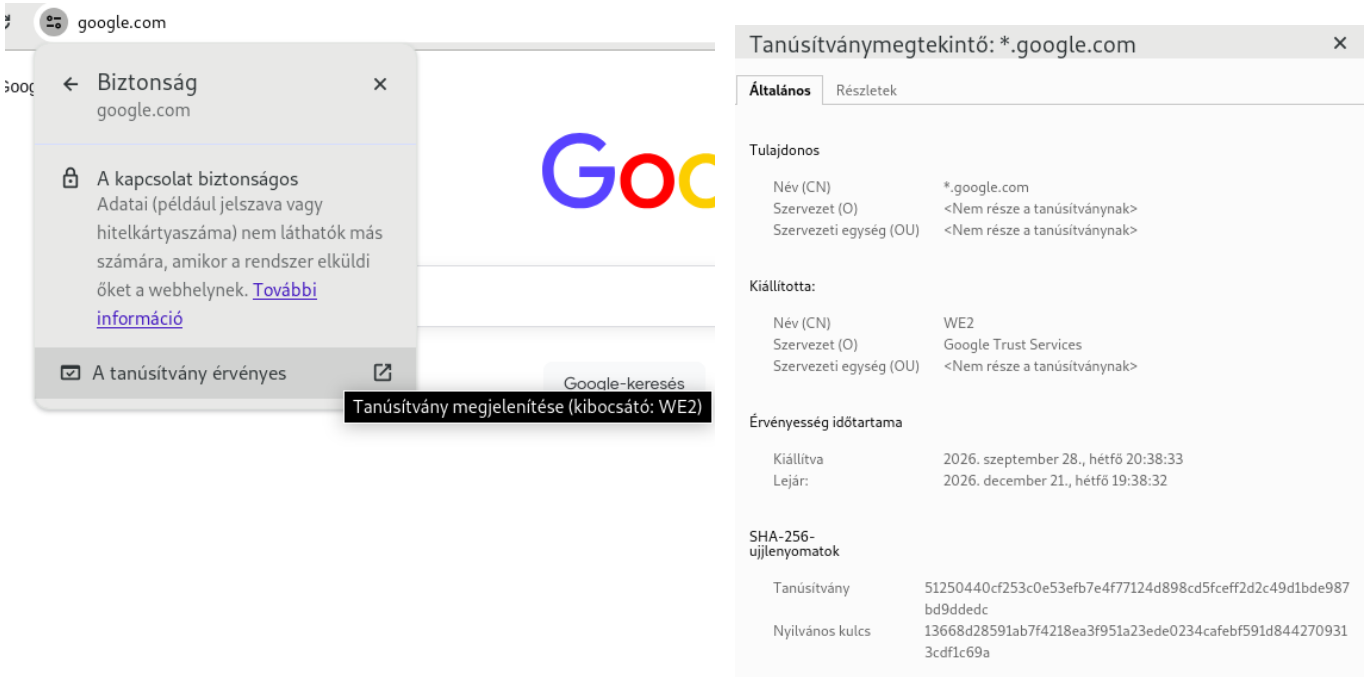
Tétel (Prímszámtétel)

Legyen n pozitív egész, és $\pi(n)$ az 1-től n-ig terjedő prímek száma. Ekkor, ahogy n tart a végtelenbe:

$$\pi(n) \approx \frac{n}{\log n}$$

RSA kódolás (Rivest, Shamir, Adleman – 1977)

- Válasszunk két "nagy" prímet: p, q (titkosak), és legyen $N = pq$ (nyilvános).
- Legyen $1 < e < \varphi(pq)$ relatív prím $\varphi(pq)$-hez. Továbbá legyen d olyan, hogy $de \equiv 1$. (e nyilvános, d titkos)
- Ha m üzenet, az elkódolt üzenet: $c = m^e \bmod N$.
- A titkos d kulcs birtokában dekódolható: $c^d = m^{ed} \equiv m \bmod N$. (Euler-Fermat tétel, kínai maradéktétel).



Feladat

Egy RSA-kódolással titkosított üzenet az alábbi számokból áll:

$$33, 23, 30, 11, 20, 15$$

Tudjuk továbbá, hogy az RSA kód nyilvános kulcsai:

$$N = 35, \quad e = 5$$

Fejtsük meg a titkosított üzenetet az alábbi lépések mentén:

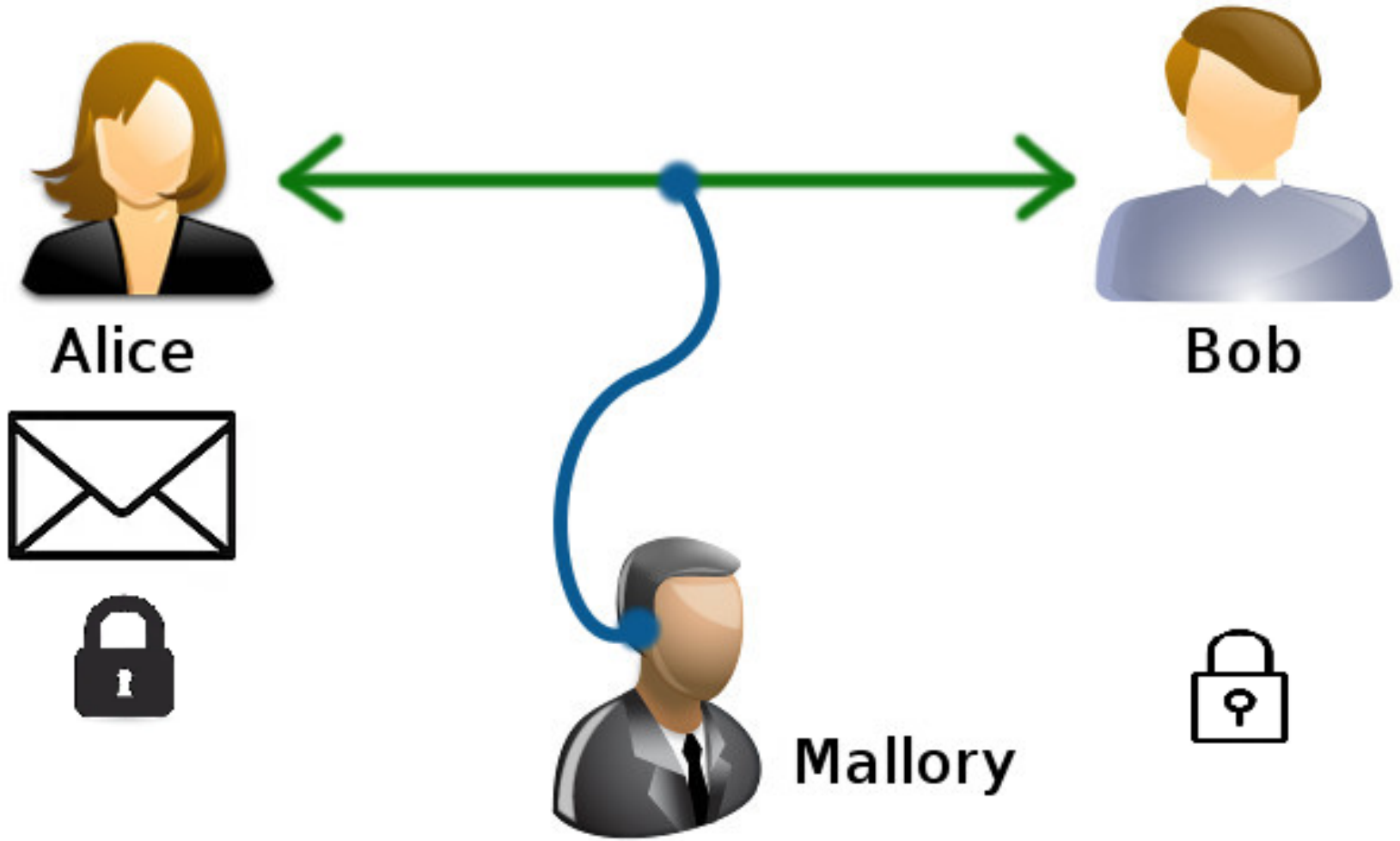
- Határozzuk meg p, q és d értékeit.
- Helyettesítsünk be $m \equiv c^d \mod N$ formulába (N, d-t már kiszámoltuk, illetve $c = 33, 23, 30, 11, 20, 15$ a kódolt karakterek)
- Az m-ekre kapott értékek az eredeti üzenet betűinek angol ábécében elfoglalt helyeit jelölik!



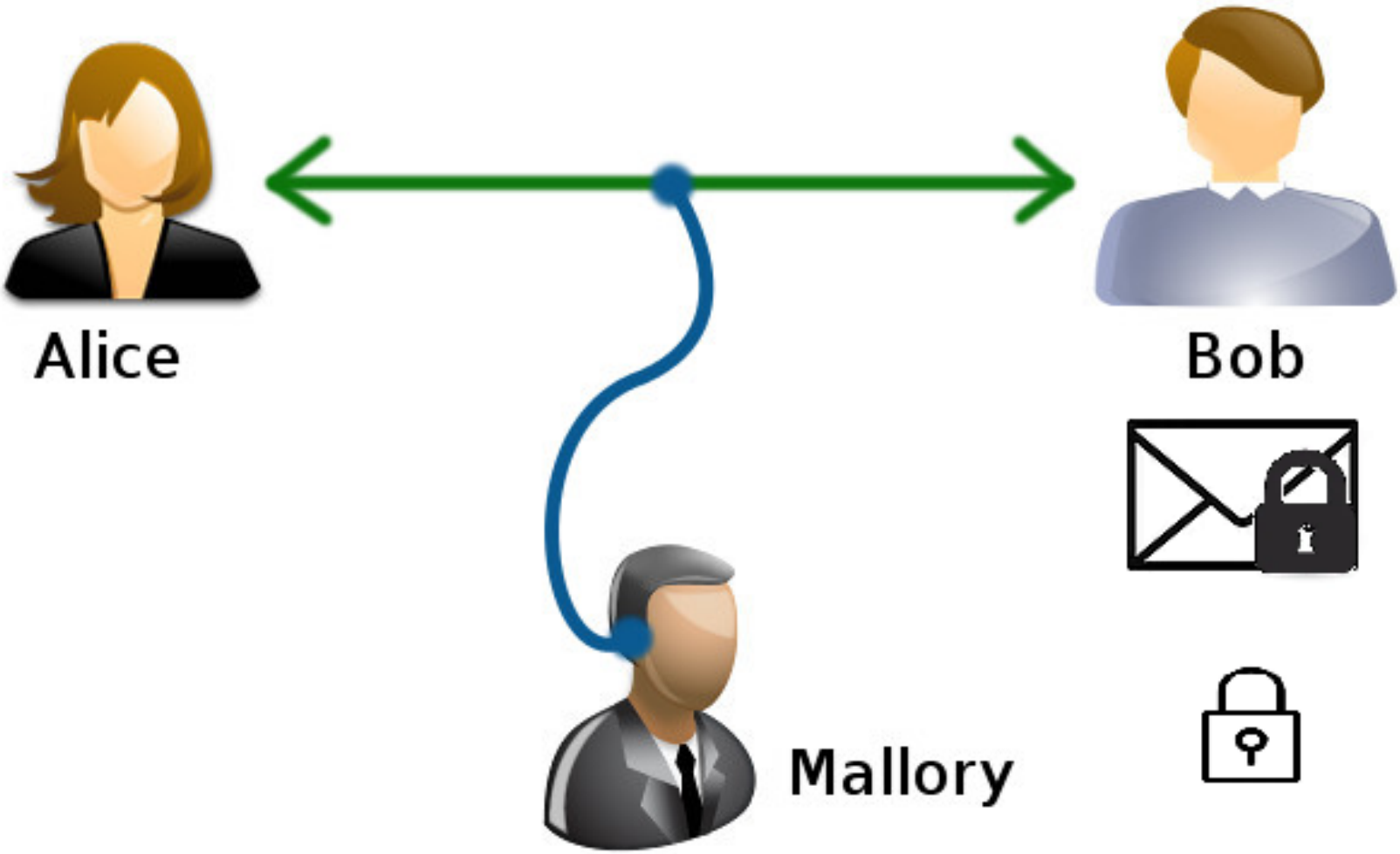
Megoldás

- $p = 5$, $q = 7$ és d olyan, hogy $5d \equiv 1 \mod 24$
- $5 \cdot 5 \equiv 25 \equiv 1 \mod 24$, tehát $d = 5$.
- $33^5 \equiv 3 \mod 35$
- $23^5 \equiv 18 \mod 35$
- $30^5 \equiv 25 \mod 35$
- $11^5 \equiv 16 \mod 35$
- $20^5 \equiv 20 \mod 35$
- $15^5 \equiv 15 \mod 35$
- $3 \to C$, $18 \to R$, $25 \to Y$, $16 \to P$, $20 \to T$, $15 \to O$

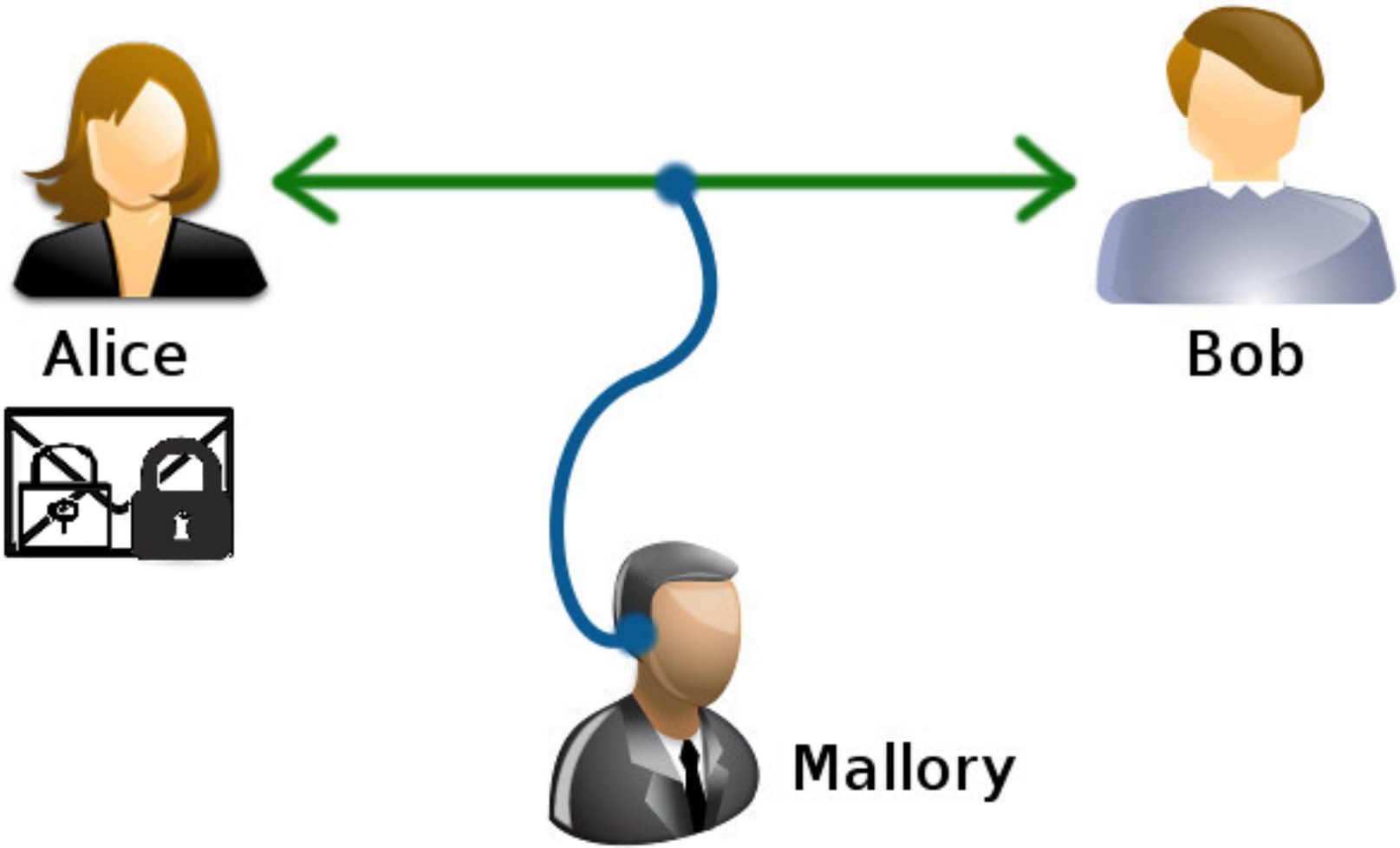
Diffie-Hellman kulcscsere



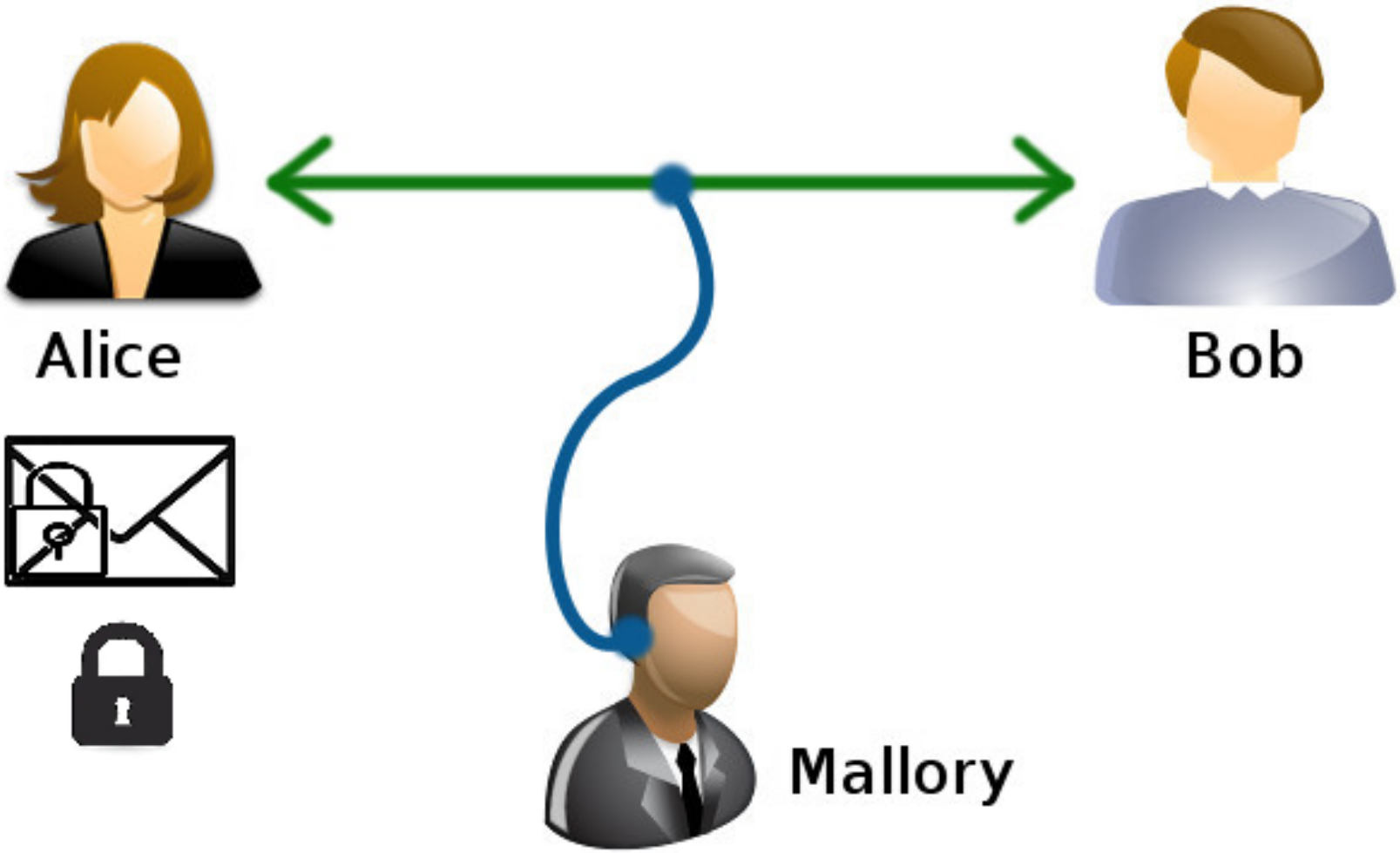
Diffie-Hellman kulcscsere



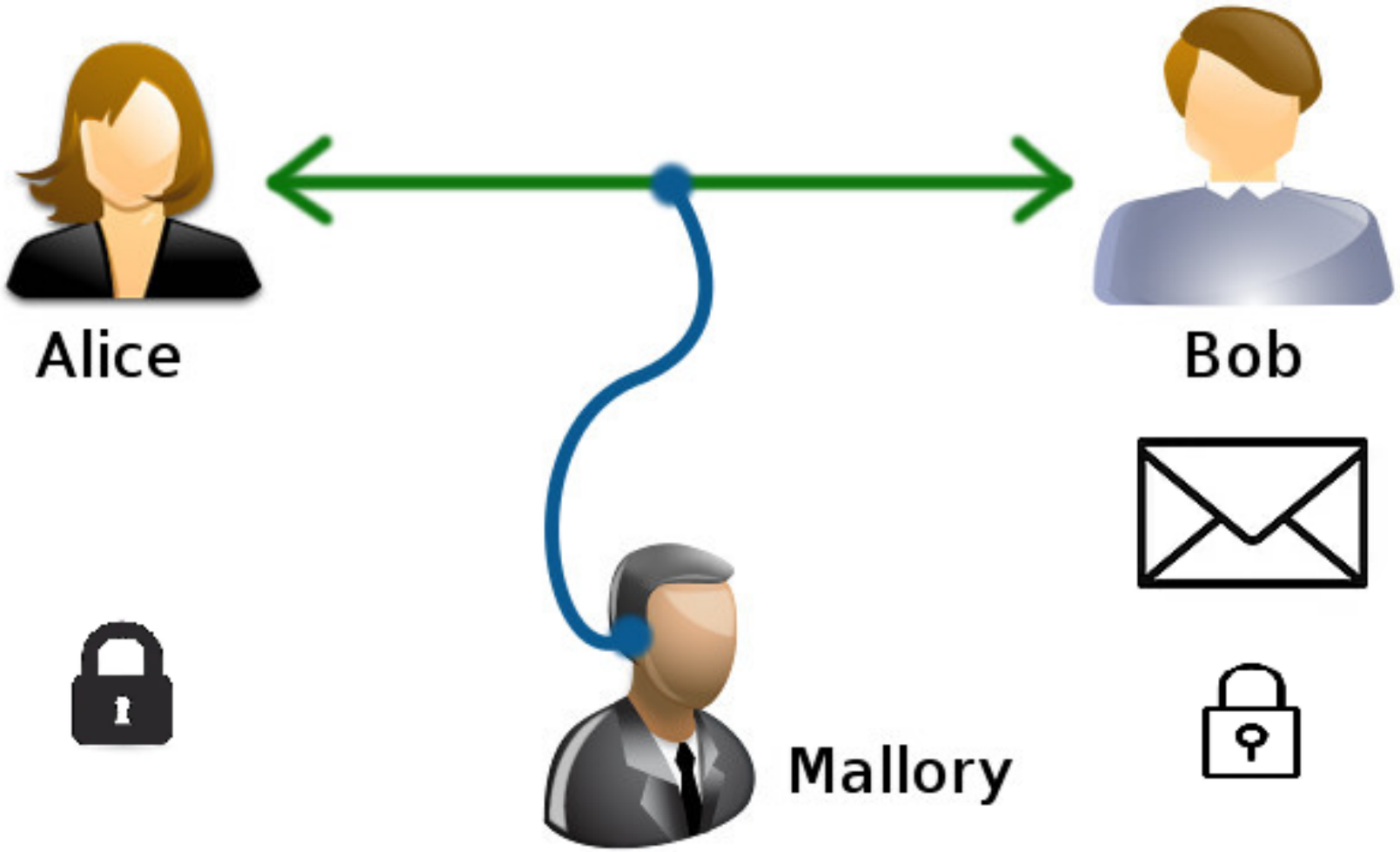
Diffie-Hellman kulcscsere



Diffie-Hellman kulcscsere



Diffie-Hellman kulcscsere

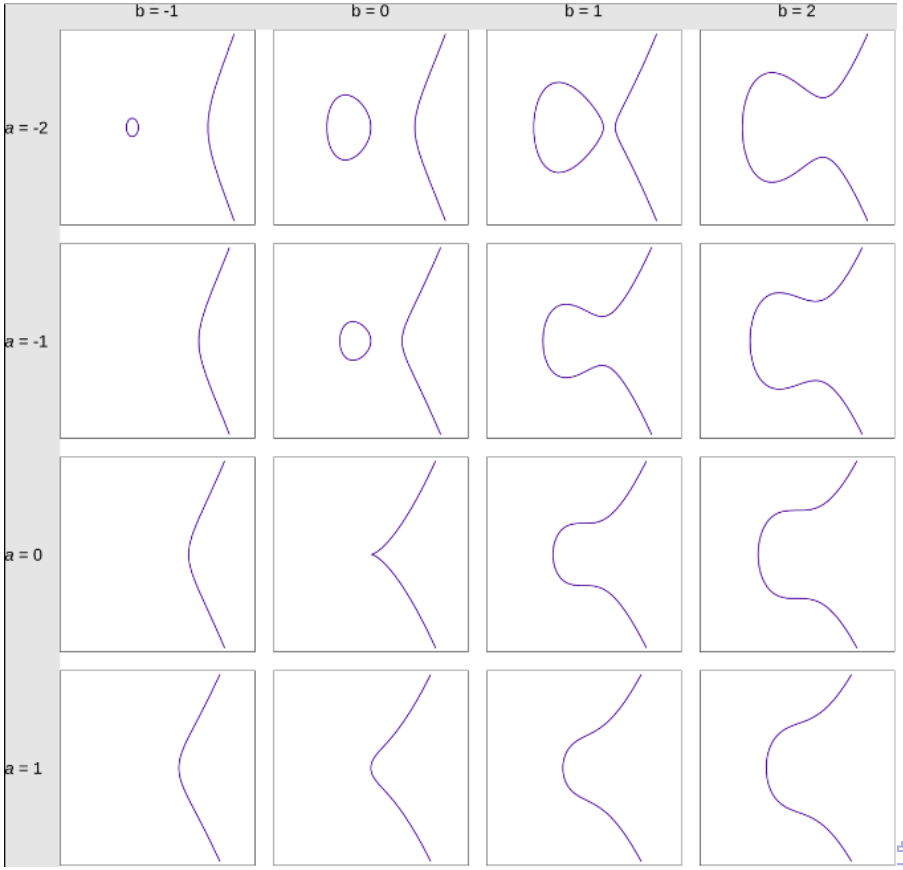


Elliptikus görbék

Definíció (Elliptikus görbe)

Harmadfokú görbe, ami sima (nincsenek csúcsai vagy önmetszései), alakja:

$$y = x^3 + Ax + B$$

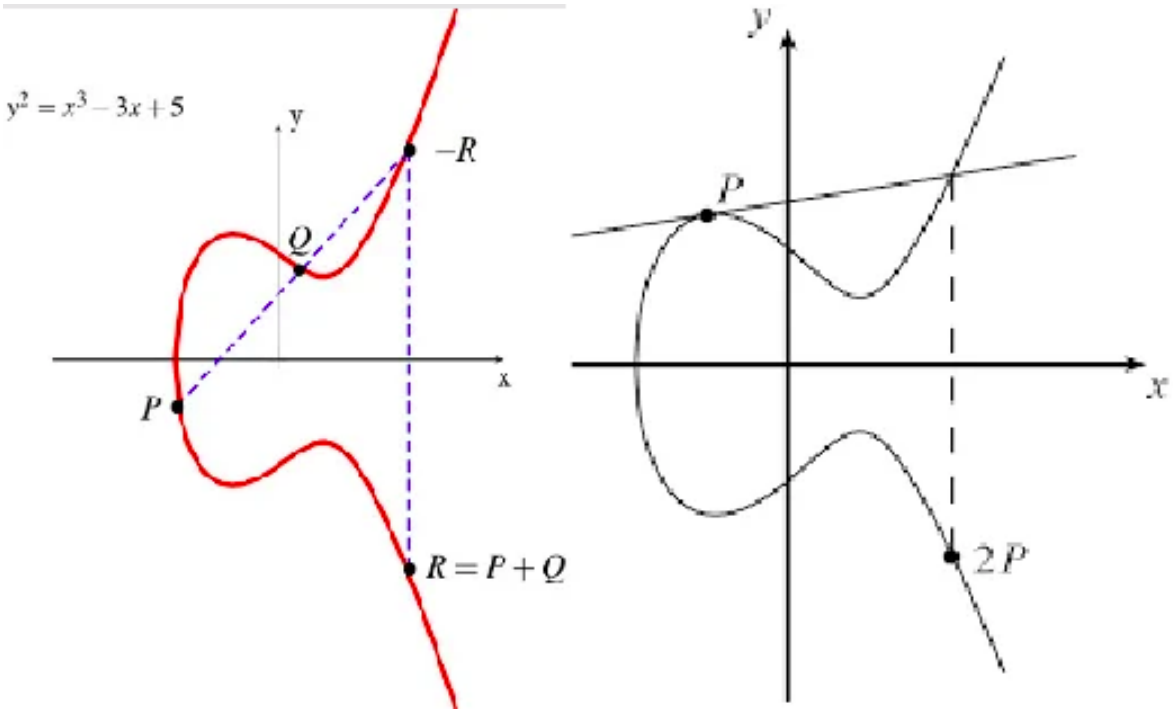


Elliptikus görbék

Tétel (Bézout-tétel)

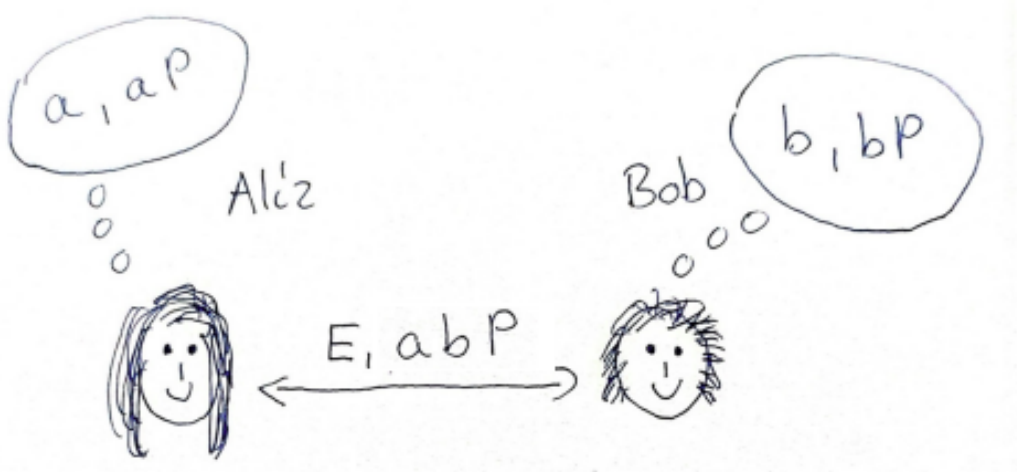
Egy elliptikus görbének és egy egyenesnek a projektív síkon, multiplicitással számolva 3 db metszéspontja van.

Összeadás elliptikus görbén:



Elliptikus görbés titkosítás

- **Titkos kulcs**: O origó
- **Üzenet**: P pont a görbén
- **Aszimmetrikus privát kulcsok**: Alice gondol egy a, Bob pedig egy b pozitív egész számra
- **Nyilvános kulcsok**: az elliptikus görbe, abP.



Példa

Digitális aláírás

Hol tartunk?

Kvantum-algoritmusok: "gyorsan" (polinom időben) tudja számolni:

- prímtényezőkre bontás (RSA) - **Shor-algoritmus**
- diszkrét logaritmus probléma (elliptikus görbés titkosítás)

Poszt-kvantum kriptográfia:

- Rács-alapú / Kód -alapú / Hash -alapú kriptográfia
- ... stb.

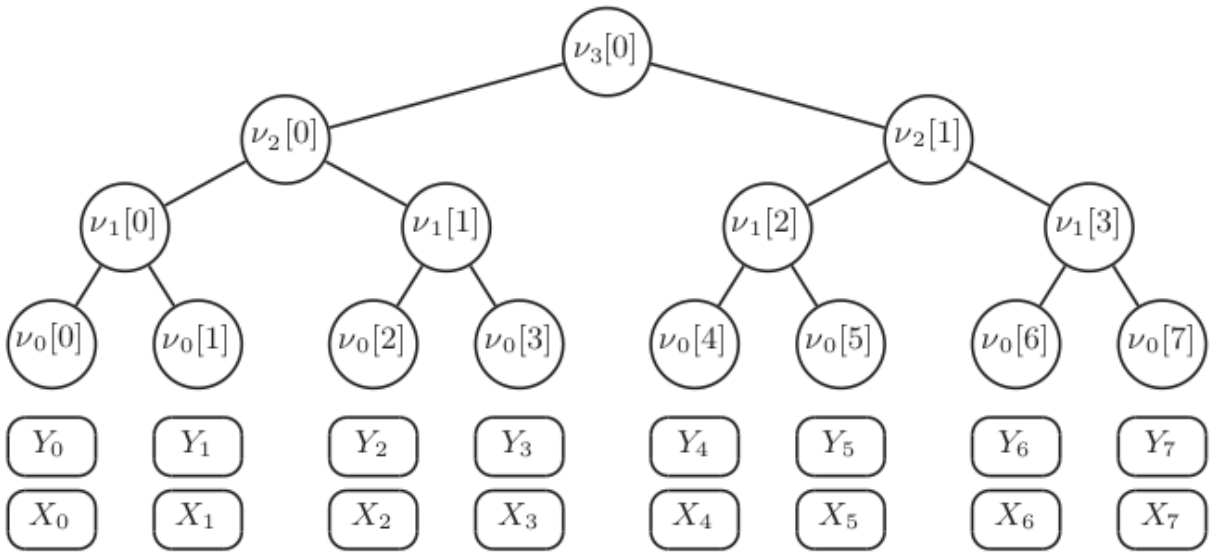


Fig. 1. A Merkle tree of height $H = 3$

MSS key pair generation requires the computation of 2^H one-time key pairs and $2^{H+1} - 1$ evaluations of the hash function.

Máig meg nem fejtett kódok

Példák: Voynich-kézirat, Shugborough-i felirat





Feladat

Problem 1. «POLY»

During a job interview, Bob was proposed to think up a small cryptosystem that operates with integers. Bob invented and implemented a complex algorithm POLY that can be represented mathematically as a polynomial. Namely, if x is a plaintext, then ciphertext y is equal to $p(x)$, where p is a polynomial with integer coefficients.

Bob's employer decided to test it. At first, he encrypted the number 20 and obtained the number 7. Secondly, he encrypted the number 15 and obtained the number 5. After that he said to Bob that there was a mistake in the implementation of the algorithm and did not hire him. What was wrong?



Megoldás

$$y = p(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_2 x^2 + a_1 x + a_0$$

Ahol $a_n, a_{n-1}, \ldots, a_1, a_0$ egész számok.

Példa

Legyen $p(x) = 5x^3 - 11x^2 + 6x - 7$, *ekkor ha az üzenet amit küldeni szeretnénk* $10111_2 = 23_{10}$, *akkor* $p(23) = 55147_{10} = 1101011101101011_2$ *a kódolt üzenet.*

A feladat szerint $p(20) = 7$ és $p(15) = 5$, tehát

$$7 = p(20) = a_n 20^n + a_{n-1} 20^{n-1} + \ldots + a_1 20 + a_0$$

A bal oldalon 7 nem osztható 5-el, $a_n 20^n + a_{n-1} 20^{n-1} + \ldots + a_1 20$ osztható 5-el, tehát a_0 nem osztható 5-el. Másrészt

$$5 = p(15) = a_n 15^n + a_{n-1} 15^{n-1} + \ldots + a_1 15 + a_0$$

A bal oldalon 5 osztható 5-el, $a_n 15^n + a_{n-1} 15^{n-1} + \ldots + a_1 15$ osztható 5-el, tehát a_0 osztható 5-el. Ellentmondás.

Feladat

Read the hidden message!



Feladat

2. Can you crack a conundrum? Below is the conundrum sent by Alice to Bob. Find an answer to Alice's question!

b tn ztwobfc twxfc t hutek vptbwbfc t svbeo hukbfq nu vx ntpo xlv
wbfus b ztwo 6 nuvpus fxpvk vkuf 2 nuvpus zusv 5 nuvpus utsv 6 nuvpus sxlvk
3 nuvpus utsv 6 nuvpus fxpvk 4 nuvpus utsv 3 nuvpus sxlvk 3 nuvpus zusv
3 nuvpus fxpvk 6 nuvpus sxlvk 3 nuvpus fxpvk 4.24 nuvpus sxlvkutsv
3 nuvpus utsv 1 nuvpu zusv 6 nuvpus fxpvk 1 nuvpu zusv 3 nuvpus utsv
6 nuvpus sxlvk 6 nuvpus fxpvk 6.49 nuvpus sxlvksxlvkutsv 6 nuvpus fxpvk
4 nuvpus utsv 3 nuvpus zusv 6 nuvpus sxlvk 3 nuvpus utsv 3 nuvpus fxpvk tfq
1 nuvpu zusv zktv bs vku ftnu vktv b ktau zpbvvuf bf vku stfq?