MATEMATICA ÎN CRIPTOGRAFIE

Profesor îndrumător: **Lector dr. Dorin Iordache**
Realizat de: **Ioniță Alin-Robert**

Facultatea de Matematică și Informatică
Specializarea Matematică-Informatică
Anul II

CUPRINS

1. Criptografie - Scop. Exemple.

Criptografia este esențială pentru securitatea cibernetică modernă și reprezintă unul dintre pilonii ce susțin protejarea vieții digitale a oamenilor.

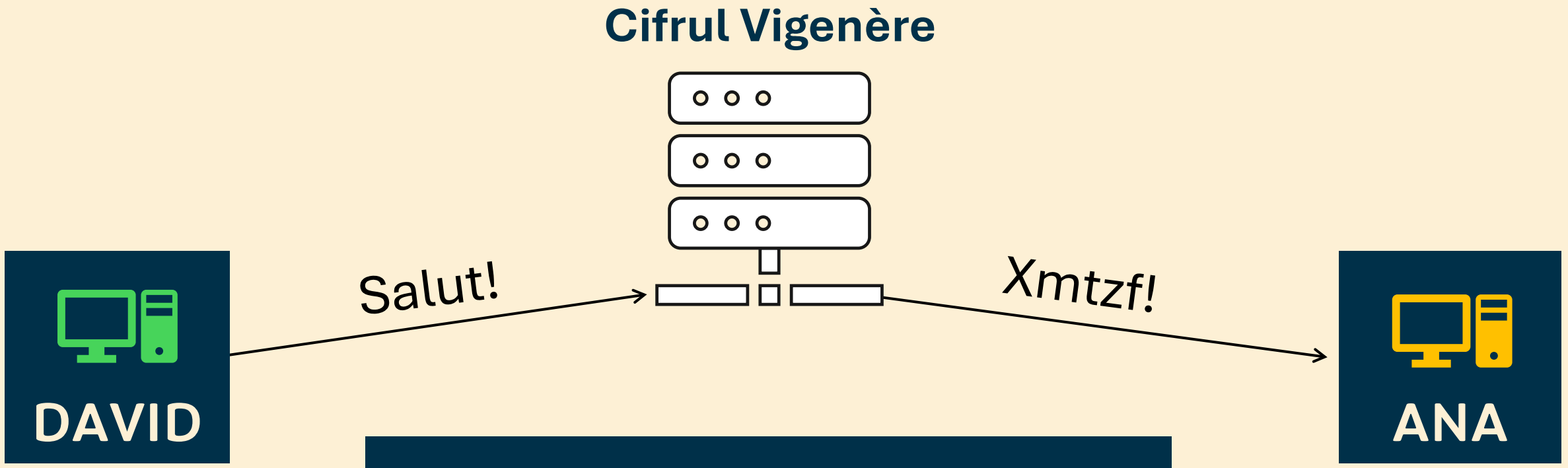
AUTENTICITATE

INTEGRITATE

CONFIDENȚIALITATE

PROTECȚIE

II. Criptarea simetrică



Exemplu: Cifrul Vigenère
Cheie: FMI

II. Criptarea simetrică

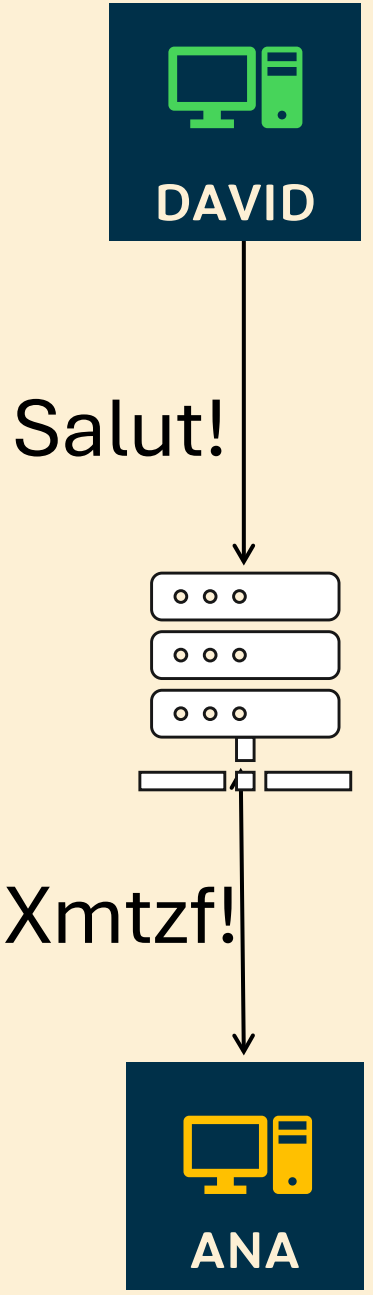
$$f(c) = (c + k) \pmod{26}$$

c = poziția din alfabet a # literei din cuvânt

k = poziția din alfabet a # literei din cheia ext.

	18	0	11	20	19
Cuvânt inițial:	S	a	l	u	t
	5	12	8	5	12
Cheie extinsă:	F	M	I	F	M

Exemplu: Cifrul Vigenère
Cheie: FMI



II. Criptarea asimetrică

I: Se aleg două numere prime mari
p = 107, q = 227

II: Se calculează modulul
n = p * q = 24289 si
O(n) = (p-1) * (q-1) = 23956
Fie e = 101 un număr coprim cu O(n)

III: Calculăm d astfel încât
e * d = 1 (mod 23956)
=> d = 20161

IV: Criptăm/Decriptăm

Exemplu: Cifrul Rivest-Shamir-Adleman (RSA)
Cheie publică: (e, n) || Cheie privată: (d, n)

II. Criptarea asimetrică

IV: Criptăm/Decriptăm

n = 24289, O(n) = 23956
e = 101, d = 20161

Criptare: $f(c) = ASCII(c)^e \pmod n$
Decriptare: $F(c) = f^d(c) \pmod n$

Criptare/Decriptare: “FMI” <--> (22459, 586, 20307)

Exemplu: Cifrul Rivest-Shamir-Adleman (RSA)
Cheie publică: (e, n) || Cheie privată: (d, n)

Funcții hash

1. Logarea în conturi

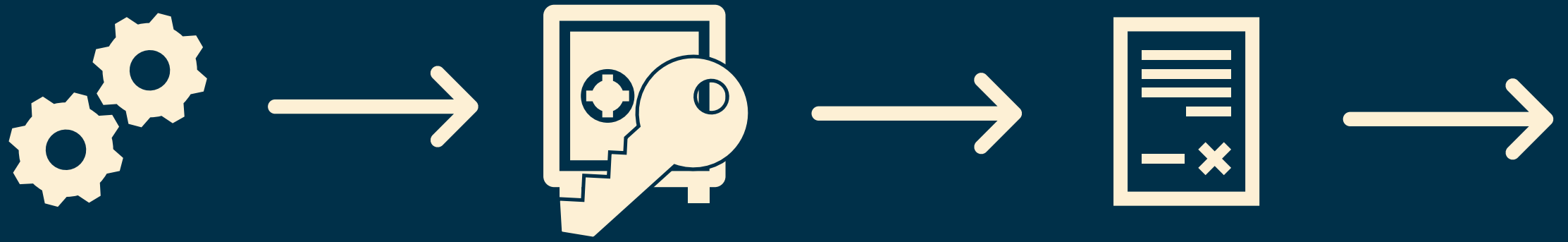
Sistemele de conturi compară, defapt, hash-ul parolei contului cu hash-ul cuvântului introdus. Logarea este permisă în cazul în care acestea sunt Identice.

"FMI" → 4f371e00f34714ee2a1022685078258 9f6b7d...

Exemplu: Secure Hash Algorithm (SHA-256)

Funcții hash

2. Semnături digitale



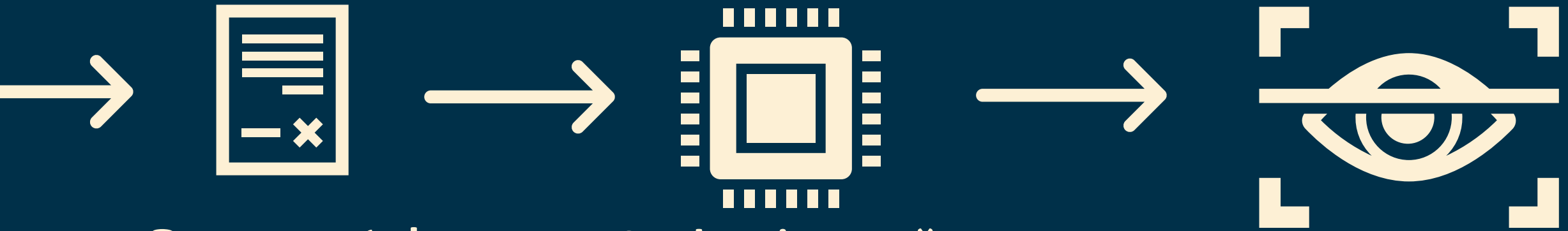
Se aplică un algoritm hash peste document

Se criptează hash-ul cu cheia privată a distribuitorului

Documentul este semnat!

Funcții hash

2. Semnături digitale



Documentul este semnat!

Se decriptează folosind cheia publică a distribuitorului

Se compară cele două hash-uri

III. Funcții hash

Criptarea este ireversabilă. “Rezumatul” are mereu lungimea de 512 biți.

Salting = Se adaugă la începutul/finalul parolei un șir de caractere aleatorii.

010001100100110101001001100..000..01000110010011010100100 1

“FMI” 24 + 1 biți 423 biți de 0 64 biți

Exemplu: Secure Hash Algorithm (SHA-256)

IV. Criptare folosind curbe eliptice

$$y^2 = x^3 + Ax + B \,||\, \Delta = 4A^3 + 27B^2 \neq 0$$

Polinomul $x^3 + Ax + B$ are rădăcini distincte, fapt ce garantează curbei eliptice proprietatea de nonsingularitate.

Nonsingularitatea asigură că există o linie tangentă bine definită în fiecare punct al curbei. Acest lucru este baza criptării folosind curbe eliptice.

IV. Criptare folosind curbe eliptice

Definirea operației “+”

Fie punctele $P_1(x_1, y_1)$, $P_2(x_2, y_2)$
pe curba eliptică E: $y^2 = x^3 + Ax + B$
Vrem $P_3 = P_1 + P_2$

Fie L: y = $\lambda x + v$, linia care conectează $P_1 \to P_2$

unde $\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1}, P_1 \neq P_2 \\ \frac{3x_1^2 + A}{2y_1}, P_1 = P_2 \end{cases}$ și $v = y_1 - \lambda x_1$

IV. Criptare folosind curbe eliptice

Definirea operației “+”

Găsim intersecția lui L cu E rezolvând

$(\lambda x + v)^2 = x^3 + Ax + B,$ adică

$x^3 + Ax + B - (\lambda x + v)^2 = 0$

Știm că x_1, x_2 sunt soluții, deci calculăm

$(x - x_1)(x - x_2)(x - x_3) = 0$, adică

$x^3 - (x_1 + x_2 + x_3)x^2 + (x_1x_2 + x_1x_3 + x_2x_3)x - x_1\, x_2\, x_3 = 0$

Așadar, avem

$-\lambda^2 = -x_1 - x_2 - x_3$ deci $x_3 = \lambda^2 - x_1 - x_2$

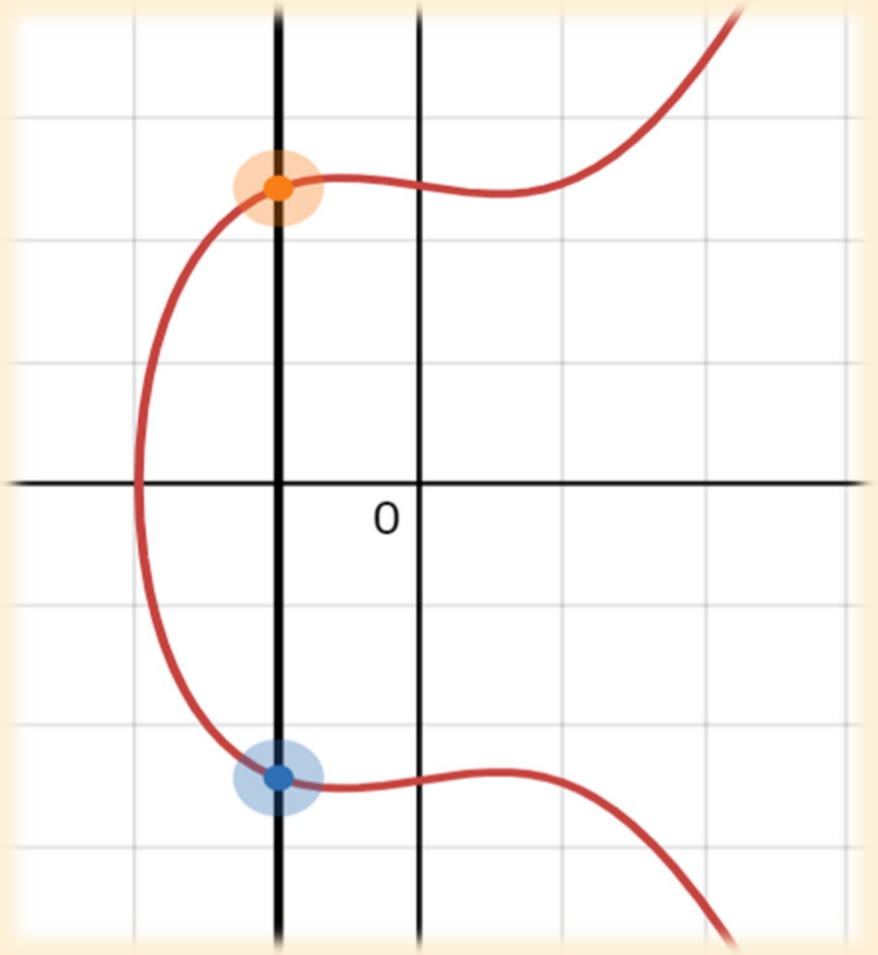
În final, calculăm y_1

$y_3 = \lambda x_3 + v$

Rezultă că P_3 are coordonatele $(x_3, -y_3)$

IV. Criptare folosind curbe eliptice

Definirea operației “+”



Formă generală

$$P_1 + P_2 = (\lambda^2 - x_1 - x_2, -\lambda^3 + \lambda(x_1 + x_2) - v)$$

Întrebare: Ce facem pentru P + (-P) ?

Soluție: Creăm un punct suplimentar Ω „la infinit”.
Regulă: Ω este un punct pe fiecare dreaptă verticală.

IV. Criptare folosind curbe eliptice

Fie E: $y^2 = x^3 - 5x + 8$

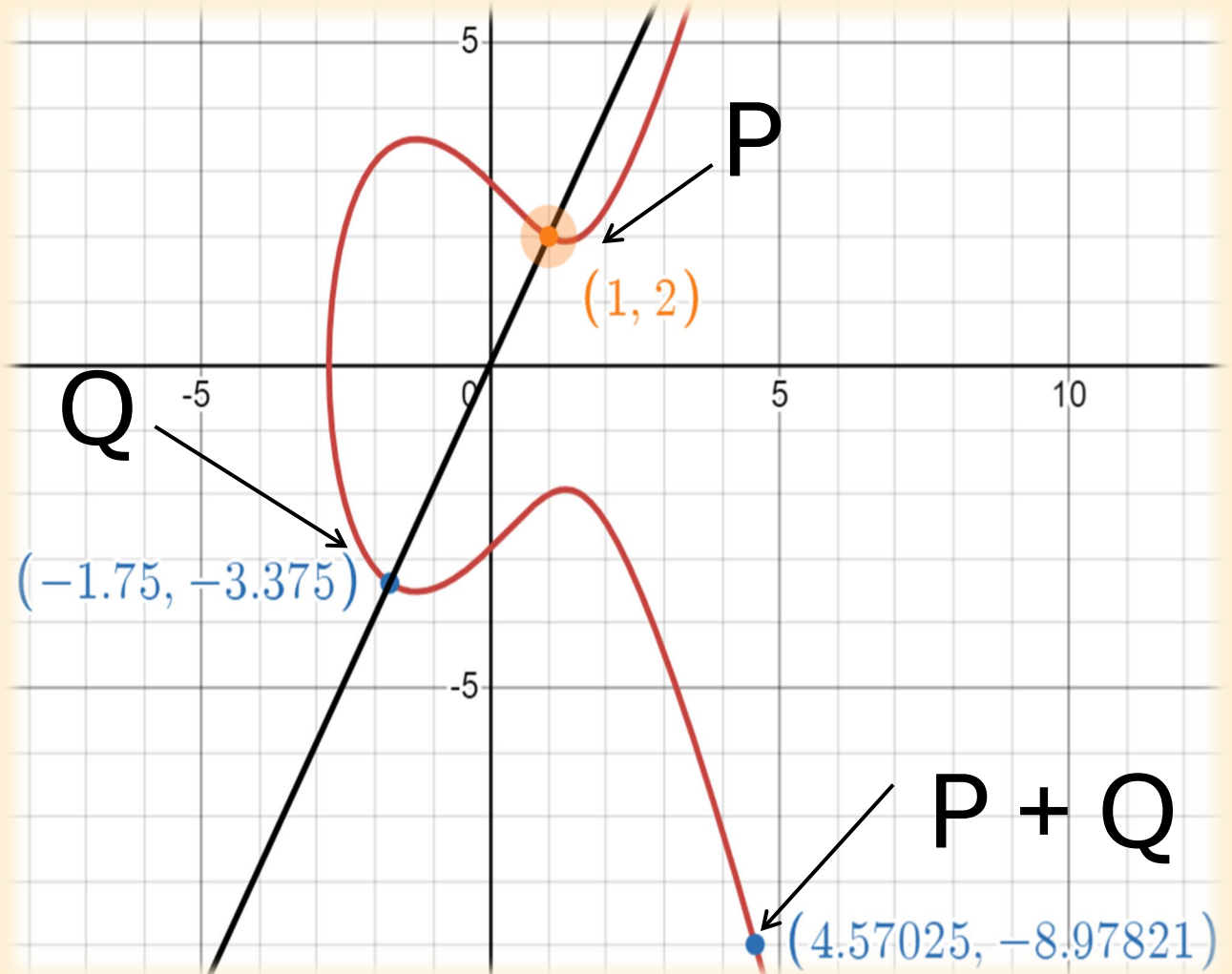
$P = (1,2)$

$2P = P + P = Q = \left(-\frac{7}{4}, -\frac{27}{8}\right)$

$3P = P + Q = \left(\frac{553}{121}, \frac{11950}{1331}\right)$

Fie $Q = 3P$

$4P = P + Q = \left(\frac{45313}{11664}, -\frac{8655103}{1259712}\right)$



IV. Criptare folosind curbe eliptice

Diffie-Hellman Key Exchange

Se stabilește o curbă eliptică E unde ECDLP este considerat foarte greu și un punct P a.î. ordinul său este un număr prim mare. După, se aplică următoarea procedură:

1. Diffie alege un a secret, calculează aP, și îl trimite lui Hellman
2. Hellman alege un b secret, calculează bP, și îl trimite lui Diffie
3. Diffie calculează bP * a = abP, Hellman calculează aP * b = abP

Ambii membrii extrag cheia privată folosind o metodă prestabilită.


Vă mulțumesc
pentru atenție!

Bibliografie:

https://www.geeksforgeeks.org/rsa-algorithm-cryptography/
https://www.geeksforgeeks.org/vigenere-cipher/
https://pages.mtu.edu/~shene/NSF-4/Tutorial/VIG/Vig-Base.html
https://www.math.brown.edu/~jhs/Presentations/WyomingEllipticCurve.pdf
https://andrea.corbellini.name/ecc/interactive/modk-add.html
https://crypto.ro/dictionar/functie-hash/
https://ro.wikipedia.org/wiki/RSA
https://www.movable-type.co.uk/scripts/sha256.html#src-code
https://www.sectigo.com/resource-library/how-digital-signatures-work
https://bearworks.missouristate.edu/cgi/viewcontent.cgi?article=4697&context=theses

Unelte folosite:

https://www.dcode.fr/rsa-cipher
https://www.asciitable.com
https://www.base64encode.org
https://www.desmos.com/calculator/ialhd71we3
https://www.calculator.net/big-number-calculator.html