CURS 13
CRIPTOGRAFIA PE CURBE ELIPTICE

- **Neal Koblitz** (University of Washington) şi **Victor Miller** (Institute for Defense Analyses - Princeton) → **1985**

- Principalul avantaj al utilizării curbelor eliptice în criptografie îl constituie asigurarea unui nivel înalt de securitate folosind chei mai scurte decât alți algoritmi similari:

Sistem de criptare simetric	Sistem bazat pe curbe eliptice	Sistemul RSA
80	160	1024
112	224	2048
128	256	3072
192	384	7680
256	512	15360

- În prezent, criptografia bazată pe curbe eliptice este utilizată în Bitcoin, Ethereum, PGP, SSH, TLS etc.

- **Curbe eliptice reale:**
  How Elliptic Curve Cryptography Works - Technical Articles (allaboutcircuits.com)

- **Curbe eliptice peste $\mathbb{Z}_p$**

  Fie $p > 3$ un număr prim.

  Curba eliptică $y^2 = x^3 + ax + b$ *peste* $\mathbb{Z}_p$ este mulțimea

$$E = \{(x, y) \in \mathbb{Z}_p \times \mathbb{Z}_p \,|\, y^2 \equiv x^3 + ax + b \pmod p\} \cup \{\mathcal{O}\}$$

  unde $4a^3 + 27b^2 \not\equiv 0 \pmod p$, iar $\mathcal{O}$ se numește *punctul la infinit*.

➢ **Exemplu:**

Fie curba eliptică $E: y^2 = x^3 + x + 5$ peste $\mathbb{Z}_{19}$.
Punctele curbei E sunt:

$$E = \{(x, y) \in \mathbb{Z}_{19} \times \mathbb{Z}_{19} | y^2 \equiv x^3 + x + 5 \pmod{19}\} \cup \{\mathcal{O}\}$$

- Calculăm y^2 pentru $y \in \mathbb{Z}_{19}$:

y	0	1	2	3	4	5	6	7	8	9
y^2	0	1	4	9	16	6	17	11	7	5

y	10	11	12	13	14	15	16	17	18
y^2	5	7	11	17	6	16	9	4	1

- Determinăm punctele curbei E:
  - $x = 0 \Rightarrow y^2 = 5 \Rightarrow y \in \{9, 10\} \Rightarrow A_1(0, 9), A_2(0, 10)$
  - $x = 1 \Rightarrow y^2 = 7 \Rightarrow y \in \{8, 11\} \Rightarrow A_3(1, 8), A_4(1, 11)$
  - $x = 2 \Rightarrow y^2 = 15 \Rightarrow y \in \emptyset$
  - $x = 3 \Rightarrow y^2 = 16 \Rightarrow y \in \{4, 15\} \Rightarrow A_5(3, 4), A_6(3, 15)$
  - $x = 4 \Rightarrow y^2 = 16 \Rightarrow y \in \{4, 15\} \Rightarrow A_7(4, 4), A_8(4, 15)$
  - $x = 5 \Rightarrow y^2 = 2 \Rightarrow y \in \emptyset$
  - $x = 6 \Rightarrow y^2 = 18 \Rightarrow y \in \emptyset$
  - $x = 7 \Rightarrow y^2 = 13 \Rightarrow y \in \emptyset$
  - $x = 8 \Rightarrow y^2 = 12 \Rightarrow y \in \emptyset$
  - $x = 9 \Rightarrow y^2 = 2 \Rightarrow y \in \emptyset$
  - $x = 10 \Rightarrow y^2 = 8 \Rightarrow y \in \emptyset$
  - $x = 11 \Rightarrow y^2 = 17 \Rightarrow y \in \{6, 13\} \Rightarrow A_9(11,6), A_{10}(11, 13)$
  - $x = 12 \Rightarrow y^2 = 16 \Rightarrow y \in \{4, 15\} \Rightarrow A_{11}(12, 4), A_{12}(12, 15)$
  - $x = 13 \Rightarrow y^2 = 11 \Rightarrow y \in \{7, 12\} \Rightarrow A_{13}(13,7), A_{14}(13, 12)$
  - $x = 14 \Rightarrow y^2 = 8 \Rightarrow y \in \emptyset$
  - $x = 15 \Rightarrow y^2 = 13 \Rightarrow y \in \emptyset$

- $x = 16 \implies y^2 = 13 \implies y \in \emptyset$
- $x = 17 \implies y^2 = 14 \implies y \in \emptyset$
- $x = 18 \implies y^2 = 3 \implies y \in \emptyset$

În concluzie, curba E are 15 puncte:

$$E = \{ \quad \mathcal{O}, A_1(0,9), A_2(0,10), A_3(1,8), A_4(1,11), A_5(3,4),$$
$$A_6(3,15), A_7(4,4), A_8(4,15), A_9(11,6), A_{10}(11,13),$$
$$A_{11}(12,4), A_{12}(12,15), A_{13}(13,7), A_{14}(13,12)\}$$

➢ **Teorema lui Hasse (1933):**

Pentru o curbă eliptică E peste $\mathbb{Z}_p$ are loc inegalitatea:

$$p + 1 - 2\sqrt{p} \leq |E| \leq p + 1 + 2\sqrt{p}$$

Exemplu:
Pentru o curbă eliptică E peste $\mathbb{Z}_{19}$ are loc inegalitatea:

$$19 + 1 - 2\sqrt{19} \leq |E| \leq 19 + 1 + 2\sqrt{19} \implies 11 \leq |E| \leq 28$$

➢ **Grupul abelian aditiv asociat unei curbe eliptice E peste $\mathbb{Z}_p$**

Fie $P(x_1, y_1), Q(x_2, y_2) \in E$ și definim $P + Q$ astfel (toate calculele se efectuează modulo p):

- $P + \mathcal{O} = \mathcal{O} + P = P$ (deci $\mathcal{O}$ este elementul neutru al grupului)
- Dacă $Q(x_1, -y_1) \implies P + Q = Q + P = \mathcal{O} \implies Q = -P$ (deci Q este elementul simetric/opusul lui P)
- $P + Q = Q + P = R(x_3, y_3)$

$$\begin{cases} x_3 = m^2 - x_1 - x_2 \\ y_3 = m(x_1 - x_3) - y_1 \end{cases}$$

$$m = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1}, & \text{dacă } P \neq Q \\ \dfrac{3x_1^2 + a}{2y_1}, & \text{dacă } P = Q \end{cases}$$

Exemple:

Fie curba eliptică $E: y^2 = x^3 + x + 5$ peste $\mathbb{Z}_{19}$.

- $2 \cdot A_1 = A_1(0,9) + A_1(0,9) = R(x_3, y_3)$

  $m = \dfrac{3 \cdot 0^2 + 1}{2 \cdot 9} = 1 \cdot 18^{-1} (\text{mod } 19) = 18$

  $\begin{cases} x_3 = 18^2 - 0 - 0 \ (\text{mod } 19) = 1 \\ y_3 = 18(0 - 1) - 9 \ (\text{mod } 19) = -27 (\text{mod } 19) = 11 \end{cases}$

  $A_1(0,9) + A_1(0,9) = A_4(1,11) \Longrightarrow 2 \cdot A_1 = A_4$

- $3 \cdot A_1 = 2 \cdot A_1(0,9) + A_1(0,9) = A_4(1,11) + A_1(0,9) = R(x_3, y_3)$

  $m = \dfrac{9 - 11}{0 - 1} = 2 \ (\text{mod } 19) = 2$

  $\begin{cases} x_3 = 2^2 - 1 - 0 \ (\text{mod } 19) = 3 \\ y_3 = 2(1 - 3) - 11 \ (\text{mod } 19) = -15 (\text{mod } 19) = 4 \end{cases}$

  $3 \cdot A_1 = 2 \cdot A_1(0,9) + A_1(0,9) = A_4(1,11) + A_1(0,9) = A_5(3,4)$

Observație:
Punctul A_1 este generator al grupului asociat curbei eliptice E deoarece:

$A_1 = 1 \cdot A_1$	$A_6 = 12 \cdot A_1$	$A_{11} = 8 \cdot A_1$
$A_2 = 14 \cdot A_1$	$A_7 = 4 \cdot A_1$	$A_{12} = 7 \cdot A_1$
$A_3 = 13 \cdot A_1$	$A_8 = 11 \cdot A_1$	$A_{13} = 10 \cdot A_1$
$A_4 = 2 \cdot A_1$	$A_9 = 6 \cdot A_1$	$A_{14} = 5 \cdot A_1$
$A_5 = 3 \cdot A_1$	$A_{10} = 9 \cdot A_1$	$\mathcal{O} = 15 \cdot A_1$

Punctul A_1 are ordinul 15, deoarece $15 \cdot A_1 = \mathcal{O}$.

Exemple:

- $49 \cdot A_1 = (3 \cdot 15 + 4) \cdot A_1 = 3 \cdot (15 \cdot A_1) + 4 \cdot A_1 = 3 \cdot \mathcal{O} + 4 \cdot A_1 = A_7$
- $A_3 + A_{13} = 13 \cdot A_1 + 10 \cdot A_1 = 23 \cdot A_1 = 8 \cdot A_1 = A_{11}$

➢ Problema logaritmului discret pentru o curbă eliptică peste $\mathbb{Z}_p$

Fie E o curbă eliptică peste $\mathbb{Z}_p$, un punct $P \in E$ de ordin mare și punctul $Q = nP = \underbrace{P + P + \cdots + P}_{n \text{ ori}}$. Atunci $n = \log_P Q$.

- Dacă se cunosc n și P, atunci Q se calculează cu complexitatea $\mathcal{O}(\log_2 n)$.

Exemplu:

$$n = 43 = 101011_2 = 1 \cdot 2^0 + 1 \cdot 2^1 + 0 \cdot 2^2 + 1 \cdot 2^3 + 0 \cdot 2^4 + 1 \cdot 2^5$$

$$Q = nP = 43P$$

T (multiplii lui P)	S (suma curentă)	Bit curent	
—	0	—	
$T = P$	$S = S + T = P$	1	$\log_2 n = 6$ pași
$T = 2T = T + T = 2P$	$S = S + T = 3P$	1	
$T = 2T = T + T = 4P$	—	0	
$T = 2T = T + T = 8P$	$S = S + T = 11P$	1	
$T = 2T = T + T = 16P$	—	0	
$T = 2T = T + T = 32P$	$S = S + T = 43P$	1	

- Dacă se cunosc P și Q, atunci complexitatea celor mai buni algoritmi pentru calculul lui n, adică a logaritmului discret al unui punct de pe o curbă eliptică peste $\mathbb{Z}_p$, Baby-step giant-step, Pohlig–Hellman, Pollard's rho, Index calculus algorithm este $\mathcal{O}(\sqrt{p}) \approx \mathcal{O}(2^{[\log_2 p]/2})$, deci este o complexitate exponențială!!!

➢ Algoritmul de criptare ElGamal pentru o curbă eliptică peste $\mathbb{Z}_p$

▪ Algoritmul de generare a cheilor:

- Se selectează un număr natural p care să fie o putere a unui număr prim, o curbă eliptică E peste $\mathbb{Z}_p$ și un punct $P \in E$ de ordin mare
- Se selectează un număr $n \in \mathbb{Z}_p^*$ și se calculează $Q = nP$, deci $n = \log_P Q$
- Cheia publică este tripletul (E, P, Q), iar cheia privată este numărul n

▪ Algoritmul de criptare:

- Presupunem că Alice are cheia publică (E, P, Q) și cheia privată n
- Bob criptează un mesaj M pentru Alice astfel:
  - alege un număr aleatoriu $r \in \mathbb{Z}_p^*$ (*cheie efemeră*)
  - criptează mesajul clar M, codificat printr-un punct de pe curba eliptică E, prin perechea:

$$C = \left(\underbrace{r \cdot P}_{A}, \underbrace{M + r \cdot Q}_{B} \right)$$

▪ Algoritmul de decriptare:

- Alice decriptează un mesaj criptat $C = (A, B)$ astfel:

$$D = B - n \cdot A$$

▪ Corectitudinea algoritmului:

Fie un mesaj criptat $C = \left(\underbrace{r \cdot P}_{A}, \underbrace{M + r \cdot Q}_{B} \right)$, rezultă că mesajul decriptat este

$$D = B - n \cdot A = \underbrace{M + r \cdot Q}_{B} - n \cdot \underbrace{r \cdot P}_{A} = M + r \cdot \underbrace{n \cdot P}_{Q} - n \cdot r \cdot P = M.$$