

CRİPTOGRAFIA PE CURBE ELIPTICE

Sistemul de Criptare ElGamal

I. Descrierea sistemului de criptare ElGamal.

II. Criptare/Decriptare

- i. Cheia publică a destinatarului este ($p=1367; \alpha=7; \beta=1146$);
- ii. Cheia privată este $a=451$;
- iii. Criptați mesajul **333** folosind $k=777$.
- iv. Decriptați mesajul $(y_1, y_2) = (1282, 59)$.
- v. Ce observați?

III. Utilizarea multiplă a lui k

- i. Cheia publică a lui Bob este ($p=83; \alpha=3; \beta=23$);
- ii. Oscar interceptează mesajul criptat $(y_1, y_2) = (17, 49)$ pe care Alice îi trimite lui Bob și știe că acestuia îi corespunde mesajul clar 11.
- iii. Oscar interceptează apoi mesajul $(y'_1, y'_2) = (17, 15)$ pe care Alice îl trimite ulterior lui Bob;
- iv. Oscar determină textul clar corespunzător celui de-al doilea mesaj. Care este acesta? (Indiciu: $49^{-1} \pmod{83} = 61$)
- v. Care este greșeala făcută de Alice care îi permite lui Oscar să realizeze decriptarea?

Curbe eliptice

I. Ce sunt curbele eliptice?

II. Numărul de puncte ale unei curbe eliptice

- i. Fie curba eliptică $y^2 = x^3 + 15x + 15$, peste \mathbb{Z}_{11} ;
- ii. Câte puncte are această curbă eliptică?
- iii. Care sunt acestea?

III. Adunarea punctelor pe curbe eliptice

- i. Fie curba eliptică $y^2 = x^3 + 21x + 7$, peste Z_{23} ;
- ii. Adunați $P = (14, 3)$ cu $Q = (6, 21)$.
- iii. Determinați $2P$.
- iv. Găsiți perechi de puncte (P, Q) care prin adunare dau O .
- v. Ce particularitate au aceste perechi?

ElGamal pe curbe eliptice

I. Descrierea sistemului de criptare ElGamal pe curbe eliptice.

II. Criptare/Decriptare

- i. Fie curba eliptică $E: y^2 = x^3 + 7x + 17$, peste Z_{31} .
- ii. Cheia secretă este $a=7$.
- iii. Cheia publică este $(\alpha = (21, 30), \beta = (21, 1), E)$.
- iv. Criptați mesajul $(21, 30)$ folosind $k=3$.
- v. Decriptați mesajul $(y_1, y_2) = ((21, 1), (30, 3))$.
- vi. Ce observați?

III. Texte clare

- i. Folosiți cheia publică de la exercițiul II.
- ii. Se poate cripta valoarea $(25, 25)$? Justificați.

IV. Alegerea curbei eliptice

- i. Se dorește alegerea unei curbe eliptice în vederea folosirii sistemului ElGamal pe grupul punctelor acestei curbe eliptice.
- ii. Găsiți un motiv pentru care curba folosită la exercițiul II nu este utilizabilă în practică.

V. Alegerea lui k

- i. Fie curba eliptică $E: y^2 = x^3 + 10x + 5$, peste Z_{23} .
- ii. Cheia publică este $(\alpha = (7, 21), \beta = (16, 12), E)$.
- iii. S-a interceptat mesajul $(y_1, y_2) = ((7, 21), (3, 4))$.
- iv. Care este mesajul clar corespunzător?

① Mai multe informații:

1. CrypTool Portal (Cryptool 1.4.30)

<http://www.cryptool.com/>

2. Interactive Security Script

<http://www2.informatik.uni-halle.de/dasi/English/english.html>

3. Modular inversion

<http://www.cs.princeton.edu/~dsri/modular-inversion-answer.php?n=18&p=47>