

## CRİPTOGRAFIA PE CURBE ELIPTICE

### Sistemul de Criptare ElGamal

#### I. Descrierea sistemului de criptare ElGamal.

#### II. Criptare/Decriptare

- i. Cheia publică a destinatarului este  $(p=2579; \alpha=2; \beta=2400)$ ;
- ii. Cheia privată este  $a=123$ ;
- iii. Criptați mesajul **1324** folosind  $k=853$ .
- iv. Decriptați mesajul  $(y_1, y_2) = (1580, 342)$ .
- v. Ce observați?

#### III. Utilizarea multiplă a lui $k$

- i. Cheia publică a lui Bob este  $(p=23; \alpha=2; \beta=18)$ ;
- ii. Oscar interceptează mesajul criptat  $(y_1, y_2) = (13, 19)$  pe care Alice îi trimite lui Bob și știe că acestuia îi corespunde mesajul clar 7.
- iii. Oscar interceptează apoi mesajul  $(y'_1, y'_2) = (13, 9)$  pe care Alice îl trimite ulterior lui Bob;
- iv. Oscar determină textul clar corespunzător celui de-al doilea mesaj. Care este acesta?
- 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  $y^2 = x^3 + 11x + 20$ , peste  $\mathbb{Z}_5$ ;
- ii. Câte puncte are această curbă eliptică?
- iii. Care sunt acestea?

### III. Adunarea punctelor pe curbe eliptice

- i. Fie curba eliptică  $y^2 = x^3 + 11x + 20$ , peste  $Z_{23}$ ;
- ii. Adunați  $P = (10, 7)$  cu  $Q(15, 15)$ .
- 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  $E: y^2 = x^3 + 11x + 20$ , peste  $Z_{23}$ .
- ii. Cheia publică este  $(\alpha = (10, 16), \beta = (22, 10), E)$ .
- iii. Cheia secretă este  $a=7$ .
- iv. Criptați mesajul  $(10, 16)$  folosind  $k=3$ .
- v. Decriptați mesajul  $(y_1, y_2) = ((2, 2), (20, 12))$ .
- vi. Ce observați?

#### III. Texte clare

- i. Folosiți cheia publică de la exercițiul II.
- ii. Se poate cripta valoarea  $(3, 5)$ ? 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  $E: y^2 = x^3 + 11x + 20$ , peste  $Z_{23}$ .
- ii. Cheia publică este  $(\alpha = (10, 16), \beta = (21, 6), E)$ .
- iii. S-a interceptat mesajul  $(y_1, y_2) = ((10, 16), (15, 15))$ .
- iv. Care este mesajul clar corespunzător?

① Mai multe informații:

1. CrypTool Portal (Cryptool 1.4.30)  
<https://www.cryptool.org/en/>
2. Interactive Cryptology Script  
<http://users.informatik.uni-halle.de/~ahyjb/krypto/>
3. Wolfram, Modular multiplicative inverse  
<https://www.wolframalpha.com/widgets/view.jsp?id=680a55df94d709f3d5a8cbcea6ccd6b0>
4. Elliptic Curves over Finite Fields  
<https://graui.de/code/elliptic2/>