CRIPTOGRAFIA PE CURBE ELIPTICE

Sistemul de Criptare ElGamal

I. Descrierea sistemului de criptare ElGamal.

II. Criptare/Decriptare

i. Cheia publică a destinatarului este **(p= 1439;α=3; β= 1091)**;
ii. Cheia privată este **a=121;**
iii. Criptaţi mesajul **1234** folosind **k=127**.
iv. Decriptaţi mesajul **(y_1, y_2) = (9, 747).**
v. Ce observaţi?

III. Utilizarea multiplă a lui k

i. Cheia publică a lui Bob este **(p= 227; α =2; β = 46);**
ii. Oscar interceptează mesajul criptat **(y_1,y_2) = (93, 197)** pe care Alice îi trimite lui Bob şi ştie că acestuia îi corespunde mesajul clar 11.
iii. Oscar interceptează apoi mesajul **(y'_1,y'_2) = (93, 167)** pe care Alice îl trimite ulterior lui Bob**;**
iv. Oscar determină textul clar corespunzător celui de-al doilea mesaj. Care este acesta? (Indiciu: $197^{-1}(\text{mod } 227)= 174$)
v. Care este greşeala 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 $\mathbf{y^2 = x^3 + 9x + 23}$, **peste** $\mathbf{Z_{11}}$;
ii. Câte puncte are această curbă eliptică?
iii. Care sunt acestea?

III. Adunarea punctelor pe curbe eliptice

i. Fie curba eliptică $\mathbf{y^2 = x^3 + 17x + 13}$, **peste** $\mathbf{Z_{29}}$;
ii. Adunaţi P= (9,5) cu Q(11,20) .
iii. Determinaţi 2P.
iv. Găsiţi 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:** $\mathbf{y^2 = x^3 + 7x + 9}$, **peste** $\mathbf{Z_{29}}$.
ii. Cheia secretă este a=7.
iii. Cheia publică este ($\mathbf{\alpha = (27,25)}$, $\mathbf{\beta = (7,16)}$,**E**).
iv. Criptaţi mesajul **(27,25)** folosind **k=3**.
v. Decriptaţi mesajul $\mathbf{(y_1, y_2) = ((11,24), (13,8))}$.
vi. Ce observaţi?

III. Texte clare

i. Folosiţi cheia publică de la exerciţiul II.
ii. Se poate cripta valoarea **(15,7)**? Justificaţi.

IV. Alegerea curbei eliptice

i. Se doreşte alegerea unei curbe eliptice în vederea folosirii sistemului ElGamal pe grupul punctelor acestei curbe eliptice.
ii. Găsiţi un motiv pentru care curba folosită la exerciţiul **II** nu este utilizabilă în practică.

V. Alegerea lui k

i. Fie curba eliptică **E:** $\mathbf{y^2 = x^3 + 13x + 7}$, **peste** $\mathbf{Z_{29}}$.
ii. Cheia publică este $\mathbf{(\alpha = (14,2), \beta = (28,14),E)}$.
iii. S-a interceptat mesajul $\mathbf{(y_1,y_2) = ((14,2), (5,20))}$.
iv. Care este mesajul clar corespunzător?

ⓘ Mai multe informaţii:

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