A se consulta **ghidul FMI**

Lucrare de Licență

Cuciureanu Dragoș-Adrian

Iunie 2023

Cuprins

1 Introducere **4**

2 Preliminarii și concepte de bază în Curbe Eliptice **5**

2.1 Curbe Eliptice 5

2.2 Adunarea punctelor pe Curbe Eliptice 8

2.3 Curbe Eliptice peste Câmpuri Finite 19

2.4 Adunarea punctelor pe Curbe Eliptice peste Câmpuri Finite 21

3 Preliminarii și concepte de bază în Criptografie **28**

3.1 Problema Logaritmului Discret (DLP) 28

3.2 Schimbul de chei Diffie–Hellman 32

3.3 Criptosistemul cu cheie publică ElGamal 38

3.4 Criptosistemul cu cheie publică RSA 44

4 Criptografia pe Curbe Eliptice **45**

4.1 Problema Logaritmului Discret pe Curbe Eliptice (ECDLP) 45

4.2 Schimbul de chei Diffie–Hellman pe Curbe Eliptice 45

4.3 Criptosistemul ElGamal pe curbe eliptice 50

4.4 Criptosistemul RSA cu curbe eliptice (ECRSA) 50

5 Aplicația suport **51**

5.1 Flask 51

6 Rezultate **52**

5 Bibliografie **53**

Rezumat

În această Lucrare de Licență vom aborda tematica ”Rolul algoritmilor geometrici în criptografie”, focusul fiind pus pe curbe eliptice.

Subiectul curbelor eliptice înglobează o mare cantitate de teorie matematică. Scopul acestei lucrări este de a oferi un rezumat concis al conceptelor fundamentale necesare aplicațiilor criptografice.

Acestă lucrare va fi împărțită în două părți: prima va consta într-o sinteză a teoriei, iar cea din urmă va fi o documentație a aplicației suport pe care am realizt-o, ce poate efectua diferite operații pe curbe eliptice, precum adunarea si înmultirea pe $\mathbb{R}$ și pe $\mathbb{F}_p$, dar și crearea a curbe elptice aleatoare peste un anumit câmp finit și prezentarea a diferite informații despre aceasta.

Capturile de ecran din lucrare sunt predominant realizate în aplicația suport creată la exemplele redactate, iar pentru figurile ce prezintă algoritmi au fost preluate din [1].

1 Introducere

2 Preliminarii și concepte de bază în Curbe Eliptice

2.1 Curbe Eliptice

Următoareul paragraf a fost preluat și adaptat din [2].

Definiţia 2.1. *Fie $\mathbb{K}$ un corp comutativ ($\mathbb{K}$ poate fi corpul numerelor reale $\mathbb{R}$, corpul $\mathbb{F}_p$, unde p este număr prim, sau corpul $\mathbb{F}_{p^k}$, unde p este un număr prim și $k \geq 1$.). Fie $a, b \in \mathbb{K}$ două elemente aparținând de corpul $\mathbb{K}$ și $f(X) = X^3 + aX + b$ un polinom cu coeficienți în $\mathbb{K}$. Acest polinom definește o curbă peste corpul $\mathbb{K}$:*

$$E(\mathbb{K}) = \left\{(X, Y) \in \mathbb{K}^2 : Y^2 = f(X)\right\}$$

Fie x_1, x_2, x_3 rădăcinile polinomului $f(X) = X^3 + aX + b$, atunci discriminantul său este:

$$\begin{aligned}\Delta_E =& \left[(x_1 - x_2)(x_2 - x_3)(x_3 - x_1)\right]^2 \\ =& -4a^3 - 27b^2\end{aligned}$$

Demonstraţie. Fie relațiile lui Viète pentru rădăcini:

$$\begin{aligned}x_1 + x_2 + x_3 &= 0 \\ x_1x_2 + x_2x_3 + x_3x_1 &= a \\ x_1x_2x_3 &= -b\end{aligned}$$

Derivăm $f(X)$ si obținem:

$$f'(X) = 3X^2 + a$$

Introducem rădăcinile x_1, x_2, x_3 în ecuație și cu ajutorul relațiilor lui Viète rezultă:

$$f'(x_1) = (x_1 - x_2)(x_1 - x_3)$$
$$f'(x_2) = (x_2 - x_1)(x_2 - x_3)$$
$$f'(x_3) = (x_3 - x_1)(x_3 - x_2)$$

Realizând produsul ecuațiilor anterioare și înlocuind în relațiile lui Viète obținem discriminantul curbei. □

Pentru a avea o curbă eliptică, toate rădăcinile trebuie sa fie distince una față de celelalte.

Remarca 2.2. *Polinomul f are rădăcini distince una față de celelalte, dacă și numai dacă* $\Delta_E \neq 0$.

Definiţia 2.3. *Fie* $F(X, Y) = Y^2 - X^3 - aX - b$ *și punctul* $P(x_0, y_0) \in E(\mathbb{K})$ *un punct de pe curbă. Punctul se numește singular dacă:*

$$\frac{\partial F}{\partial x}(x_0, y_0) = \frac{\partial F}{\partial y}(x_0, y_0) = 0$$

Definiţia 2.4. *O curbă* $E(\mathbb{K})$ *cu* $\Delta_E \neq 0$ *nu are puncte singulare.*

Demonstraţie. Presupunem prin absurd că o curbă $E(\mathbb{K})$ cu $\Delta_E \neq 0$ are punct singular $P(x_0, y_0)$. Acesta ar fi soluția derivaleor parțiale ale funcției $F(X, Y) = X^3 + aX + b - Y^2$. Calculăm derivatele sale parțiale:

$$\frac{\partial F}{\partial x}(x_0, y_0) = 3x_0^2 + a = 0$$
$$\frac{\partial F}{\partial y}(x_0, y_0) = -2y_0 = 0$$

Din a doua ecuație obținem că $y_0 = 0$ și introducem în $Y^2 = X^3 + aX + b$ rezulă că $x_0^3 + ax_0 + b = 0$. Iar din prima ecuație obținem $a = -3x_0^2$ și înlocuind în ecuația obținută anterior avem:

$$\begin{aligned} x_0^3 + ax_0 + b &= 0 \\ x_0^3 - 3x_0^2 x_0 + b &= 0 \\ -2x_0^3 + b &= 0 \\ b &= 2x_0^3 \end{aligned}$$

Aducând in formula discriminantului avem:

$$\begin{aligned} \Delta_E &= -4a^3 - 27b^2 \\ \Delta_E &= -4(-3x_0^2)^3 - 27(2x_0^3)^2 \\ \Delta_E &= 108x_0^6 - 108x_0^3 \\ \Delta_E &= 0 \\ dar \Delta_E \neq 0 &\Rightarrow \perp \end{aligned}$$

□

Exemplul 2.5. *Exemple de curbe care au $\Delta_E = 0$ (au puncte singulare):*

$E1 : Y^2 = X^3$ *varful de coordonate* $(0, 0)$ *este punct de inflexiune*

$E2 : Y^2 = (X + 1)^2(X - 2) = X^3 - 3x - 2$ *punctul de coordonate* $(-1, 0)$ *este izolat*

Definiţia 2.6. *Fie $\mathbb{K}$ un corp comutativ ($\mathbb{K}$ poate fi corpul numerelor reale $\mathbb{R}$, corpul*

$\mathbb{F}_p$, unde p este număr prim, sau corpul $\mathbb{F}_{p^k}$, unde p este un număr prim și $k \geq 1$.). Fie $a, b \in \mathbb{K}$ două elemente aparținând de corpul $\mathbb{K}$ și $f(X) = X^3 + aX + b$ un polinom cu coeficienți în $\mathbb{K}$. Acest polinom definește o curbă eliptică peste corpul $\mathbb{K}$:

$$E(\mathbb{K}) = \{(X, Y) \in \mathbb{K}^2 : Y^2 = f(X)\} \cup \{O\}$$
$$cu\ \Delta_E \neq 0$$

Pe scurt, putem spune că o curbă elitpică este totalitatea soluțiilor cu ecuația cu $\Delta_E \neq 0$ de forma:

$$E : Y^2 = X^3 + aX + b$$

Ecuațiile de acestă natură se cheamă ecuații *Weierstrass*.

Exemplul 2.7. *Exemple de curbe eliptice:*

$$E1 : Y^2 = X^3 - 6X + 6$$
$$E2 : Y^2 = X^3 + 3X - 1$$

Așa arată exemplele ilustrate:

2.2 Adunarea punctelor pe Curbe Eliptice

Una dintre proprietățile remarcabile ale curbelor eliptice este capacitate de a „aduna" în mod natural două puncte pe o curbă eliptică pentru a genera un al treilea punct. Înconjurăm cuvântul „aduna" între ghilimele, deoarece descriem o operație

care reunește două puncte într-un mod asemănător cu adunarea (este comutativă, asociativă și există o identitate), dar destul de diferită în alte aspecte. Geometria este cel mai natural mod de a reprezenta operația de ”adunare” pe curbe eliptice.

Fie două puncte de pe curba eliptică E: $P(x_1, y_1)$ *și* $Q(x_2, y_2)$. Trasăm dreapta ce trece prin cele 2 puncte. Cum curba eliptică este determinată de un polinom de gradul 3, dreapta desenată ca interesecta curba eliptică E în exact 3 puncte (nu este nevoie ca acestea să fie dintincte). Vom nota al treilea punct din intersecție cu $R(x_3, y_3)$, realizăm reflecția sa față de axa OX (curba eliptică E este simetrică față de axa OX) adică, din punct de vedere numeric înmulțim coordonata a doua a punctului R cu -1, acest punct va fi notat cu R' și va avea coordonatele $(x_3, -y_3)$.

Punctul R' este rezultatul ”adunării” între punctele P si Q. Pentru a nu confunda acestă operație cu adunarea naturala o vom nota cu:

$$P \oplus Q = R'$$

Exemplul 2.8. *Fie curba eliptică E de ecuație:*

$$E : Y^2 = X^3 - 7X + 10 \tag{1}$$

Și punctele $P(1, 2)$ *și* $Q(3, 4)$ *de pe E. Calculăm ecuația dreptei L ce inter-*

sectează punctele cu ajutorul pantei:

$$\begin{aligned} m &= \frac{y_2 - y_1}{x_2 - x_1} \\ &= \frac{4-2}{3-1} = 1 \\ L &: Y - y_1 = m(X - x_1) \\ L &: Y - 2 = 1(X - 1) \\ L &: Y = X + 1 \end{aligned} \tag{2}$$

Pentru a determina R' calculăm toate punctele de intersecție dintre dreapta L si curba eliptică E, substituind ecuația lui L (2) în ecuția lui E (1):

$$\begin{aligned} (X+1)^2 &= X^3 - 7X + 10 \\ X^2 + 2X + 1 &= X^3 - 7X + 10 \\ X^3 - X^2 - 9X + 9 &= 0 \end{aligned} \tag{3}$$

Cum ecuția rezultată la (3) este de gradul 3, o să aibă exact 3 rădăcini. Cum punctele $P(1,2)$ și $Q(3,4)$ sunt si pe dreaptă si pe curbă, înseamnă că 1 și 3 sunt rădăcini, deci ne rămâne de găsit doar a 3-a rădăcină (descompunem în factori):

$$\begin{aligned} X^3 - X^2 - 9X + 9 &= (X-3)(X-1)(X+3) \\ (X-3)(X-1)(X+3) &= 0 \end{aligned}$$

Din descompunerea în factori determinăm că a treia rădăcină este -3, aceasta fiind și componenta R_x, acum calculăm componeneta R_y din ecuția dreptei de la

punctul (2):

$$Y = X + 1$$
$$= (-3) + 1 = -2$$

Astfel obținem punctul R(-3, -2), tot ce rămăne de făcut pentru a obține rezultatul căutat este să reflectăm componenta R_y și obținem $R'(-3, 2)$, prin urmare:

$$P \oplus Q = (-3, 2)$$

Acesta este cazul general de adunare a două puncted de pe o curbă eliptică. Însă există și câteva cazuri particulare, fie punctul $P(x, y)$, $P' = -P = (x, -y)$ și punctul $O(\infty, \infty)$:

(i) $P \oplus P$ adunarea unui punct cu el însuși

(ii) $P \oplus P'$ adunarea unui punct cu inversul său

(iii) $P \oplus O$ adunarea unui punct cu infinit

Începem cu primul caz particular, pentru a realiza $P \oplus P$ dreapta L va fi tangenta la E, astfel dreapta intersectează curba eliptică tot în 3 puncte, doar ca 2 dintre acestea sunt P (putem să facem o paralelă cum un polinom ca $(x-1)^2$ are 2 rădăcini, chiar dacă acestea sunt identice). Al 3-lea punct va fi R și apoi calculăm R' la fel ca mai sus.

Exemplul 2.9. *Considerăm aceeași curbă eliptică E și $P(1, 2)$ de la* (1) *și calculăm $P \oplus P$:*

Determinăm panta lui E prin diferențiere în (1):

$$2Y\frac{dY}{dX} = 3X^2 - 7$$
$$\frac{dY}{dX} = \frac{3X^2 - 7}{2Y}$$

Calculăm panta lui E în P substituind P în ecuție și obținem panta $m = \frac{-4}{4} = -1$. *Astfel tangenta la E în P este:*

$$\begin{aligned} L &: Y - y_1 = m(X - x_1) \\ L &: Y - 2 = -1(X - 1) \\ L &: Y = -X + 3 \end{aligned} \tag{4}$$

Analog ca la adunarea generală, determiăm R' calculând toate punctele de intersecție dintre dreapta L si curba eliptică E, substituind ecuația lui L (4) *în ecuția lui E* (1)*:*

$$\begin{aligned} (-X + 3)^2 &= X^3 - 7X + 10 \\ X^2 - 6X + 9 &= X^3 - 7X + 10 \\ X^3 - X^2 - X + 1 &= 0 \\ (X - 1)^2(X + 1) &= 0 \end{aligned} \tag{5}$$

Observăm din descompunere ca rădăcinile sunt: -1, 1 și 1 (de remarcat că rădăcina 1, mai exact componenta P_x *apare de două ori). Cea de-a treia rădăcină este componenta* R_x*, pe care o introducem în ecuația de la (4) și obținem* $R(-1, 4)$*,*

respectiv $R'(-1,-4)$*:*

$$P \oplus P = (-1,-4)$$

Trecem la al doilea caz: $P \oplus P'$ (adunarea unui punct cu opusul său).

Definiţia 2.10. *Definim ca fiind punctul de la "infinit" punctul* $O(\infty,\infty)$.

Acest punct nu există în planul XOY. Făcând o referință la definiția care precizează că două drepte paralele se întâlnesc la "infinit", atunci considerăm că toate verticalele paralele cu OY se intersectează în punctul $O(\infty,\infty)$.

Revenind la al doilea caz, observăm că apar probleme când încercăm să adunăm la punctul $P(x,y)$, reflexia (opusul) sa față de axa OX, mai exact punctul $P' = -P = (x,-y)$. Încercăm să reărezentăm geometric adunarea ducând dreapta L prin punctele P și P', astfel creând o verticală paralelă cu OY cu X = x. Neexistând un al treilea punct al intersecției, considerăm punctul $O(\infty,\infty)$ definit anterior ca fiind rezultatul adunării.

$$P \oplus P' = O$$

Exemplul 2.11. *Considerăm aceeași curbă eliptică E de la (1) și punctele* $P(1,2)$ *și* $P'(1,-2)$ *existente pe E și calculăm* $P \oplus P'$ *ca fiind:*

$$P(1,2) \oplus P'(1,-2) = O(\infty,\infty)$$

Cazul al treilea: $P \oplus O$ (adunarea unui punct cu infinit).

Odată ce am definit punctul de la "infinit" O, trebuie să definim cum se adună un punct oarecare $P(x,y)$ de pe o curbă elitptică E împreună cu punctul O. Și această speță este mai ușor de prezentat cu ajutorul reprezentării geoemtrice. Cum punctul

O există pe fiecare verticală, putem construi dreapta L ca fiind dreapta ce trece prin punctele P și O. Dreapta L intersectează curba eliptică E în trei puncte: P, O și P'. Deci, conform algorimului de adunare definit anterior, rezultă că $R = P'$ și $R' = P$, astfel:

$$P \oplus O = P$$

Deci, punctul O este element neutru la adunarea pe curbe elitpice.

Exemplul 2.12. *Considerăm aceeași curbă eliptică E de la* (1) *și punctul* $P(1, 2)$ *existent pe E și calculăm* $P \oplus O$ *ca fiind:*

$$P(1, 2) \oplus O(\infty, \infty) = P(1, 2)$$

Pe lângă acestea mai există încă un speță particulară, care este reuniunea cazurilor 1 și 2 anterioare. Mai exact când adunăm punctul $P(x, y)$ cu el însuși și rezultă $O(\infty, \infty)$:

$$P \oplus P = O$$

Dar tocmai am arătat că:

$$P \oplus P' = O$$

Deci $P(x, y) = P'(x, -y)$, ceea ce înseamnă că $y = -y$, singura soluție validă fiind $y = 0$. Pe scurt acest caz se poate realiza doar când adunăm un punct cu el însuți și tangenta este o verticală paralelă cu OX.

Exemplul 2.13. *Fie curba eliptică E în* $\mathbb{R}$*:*

$$E : Y^2 = X^3 - 6X + 9$$

Și punctele $P(-3,0)$ și $P'(-3,0)$:

$$P(-3,0) = P'(-3,0)$$
$$P(-3,0) + P(-3,0) = P(-3,0) + P'(-3,0)$$
$$P(-3,0) + P(-3,0) = 0(\infty,\infty)$$

Definiţia 2.14. *Fie o curbă eliptică E în $\mathbb{R}$ și punctele $P(x_1,y_1)$ și $Q(x_2,y_2)$, notăm reflexia punctului față de axa OX ca fiind $P' = -P = (x_1,-y_1)$, definim scăderea ca fiind:*

$$P - Q = P \oplus (-Q) = P \oplus Q'$$

Sau direct:

$$P - Q = P + (-Q) = P + Q'$$

Exemplul 2.15. *Considerăm adunarea pe curba eliptică E în $\mathbb{R}$ și punctele $P(1,2)$, $Q(3,4)$, $Q'(3,-4)$ și R'(-3, 2) existente pe E de la Exemplul 2.8:*

$$P \oplus Q = R'$$

Deci:

$$\begin{aligned} P - Q' &= P \oplus (-Q') \\ &= P \oplus Q \\ &= R' \end{aligned}$$

Definiţia 2.16. *Fie o curbă eliptică E în $\mathbb{R}$ și punctul $P(x,y)$ de pe E și scalarul n,*

definim înmulțirea ca fiind adunarea repetată a punctului P cu el însuși de n ori:

$$n \otimes P = \underbrace{P \oplus P \oplus P \oplus ... \oplus P}_{\textit{n times}}$$

Sau direct:

$$nP = \underbrace{P + P + P + ... + P}_{\textit{n times}}$$

Exemplul 2.17. *Considerăm aceeași curbă eliptică E în $\mathbb{R}$ de la* (1)*, punctul $P(1, 2)$ existent pe E și scalarul n:*

$$\begin{aligned} 4P &= P + P + P + P \\ &= (1, 2) + (1, 2) + (1, 2) + (1, 2) \\ &= (-1, -4) + (1, 2) + (1, 2) \\ &= (9, -26) + (1, 2) \\ &= (2.25, 2.375) \end{aligned}$$

Teorema 2.18. *Fie o curbă eliptică E în $\mathbb{R}$, și fie $\mathbb{E}$ mulțimea punctelor de pe E, atunci ($\mathbb{E}$, $\oplus$) formează un grup abelian:*

1. *Asociativitate: $P + Q = P + Q + P$ pentru orice $P, Q \in \mathbb{E}$*
2. *Comutativitate: $(P + Q) + R = P + (Q + R)$ pentru orice $P, Q, R \in \mathbb{E}$*
3. *Element neutru: $P + O = O + P = P$ pentru orice $P \in \mathbb{E}$*
4. *Inversibilitate: $P + (-P) = O$ pentru orice $P \in \mathbb{E}$*

Următorul paragraf este preluat din [1].

Teorema 2.19. *Fie o curbă eliptică E:*

$$E : Y^2 = X^3 + aX + b$$

și punctele $P(x_1, y_1)$ *și* $Q(x_2, y_2)$ *de pe E, algoritmul de adunare în pseudocod este:*

(a) dacă $P = O$*, atunci* $P + Q = Q$

(b) altfel, dacă $P = O$*, atunci* $P + Q = Q$

(c) altfel, dacă $x_1 = x_2$ *și* $y_1 = -y_2$*, atunci* $P + Q = O$

(d) altfel, calculăm panta m ca fiind:

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

și fie:

$$x_3 = m^2 - x_1 - x_2$$

$$y_3 = m(x_1 - x_3) - y_1$$

rezultă:

$$P + Q = (x_3, y_3)$$

Următorul demonstrație este preluată și adaptată din [1].

Demonstraţie. Subpunctele (a) și (b) sunt prezentate anterior. Cazul (d) este atunci când linia ce trece prin P și Q este verticală, deci $P + Q = O$ (dacă $y_1 = y_2 = 0$, atunci tangenta este verticală și acest caz este acoperit de asemenea). Pentru subpunctul (e), dacă $P \neq Q$, atunci m este panta dreptei ce trece prin P și Q, altfel m este panta tangentei la $P = Q$. În ambele cazuri, dreapta L este dată de ecuația:

$$Y = mX + \nu$$

$$\nu = y_1 - mx_1$$

Substituind ecuația dreptei L în ecuția curbei E rezultă:

$$(mX + \nu)^2 = X^3 + aX + b$$

Deci:

$$X^3 - m^2X^2 + (a - 2m\nu)X + (b - \nu^2) = 0$$

Știm ca două dintre rădăcini sunt x_1 și x_2 și cum ecuația este de gradul 3 înseamnă că are 3 rădăcini. Notăm a treia rădăcină x_3 și factorizăm:

$$X^3 - m^2X^2 + (a - 2m\nu)X + (b - \nu^2) = (x - x_1)(x - x_2)(x - x_3)$$

Înmulțim partea dreaptă și ne uităm la coeficienții lui X^2 de pe ambele părți. Coeficientul din dreapta de $-x_1 - x_2 - x_3$ trebuie să fie egal cu cel din stânga $-m^2$. Astfel rezultă $x_3 = m^2 - x_1 - x_2$. Apoi obținem coordonata Y al celui de al treilea punct de intersecție dintre E și L ca fiind $mx_3 + \nu$. Pentru a obține $P + Q$ trebuie sa luăm opusul componentei Y față de axa OX și obținem $y_3 = m(x_1 - x_3) - y_1$. □

2.3 Curbe Eliptice peste Câmpuri Finite

În subcapitolele anterioare am prezentat curbele eliptice și operațiile ce se pot realiza pe acestea. Abordartea a fost predominant dintr-un punct de vedere geometric, spre exemplu, la adunarea a două puncte P și Q de pe o curbă epitică E, am tras o linie ce trece prin cele două puncte și am determinat care este ce de al treilea punct în care intersectează dreapta curba eliptică și am realizat reflexia față de axa OX. Aceasta poate fi observată în subcapitolul anterior unde am arătat cum se realizează operații pe curbe elitpice.

În criptografie se folosesc curbe eliptice peste câmpuri finite, ci nu curbe eliptice, deoarece acestea oferă garanții de securitate mai puternice și eficiență din punct de vedere computațional. Aceste proprietăți fac din criptografia cu curbe eliptice pe câmpuri finite o alegere populară în sistemele criptografice moderne. Deci, trebuie să examinăm curbele eliptice ale căror puncte au coordonate într-un câmp finit $\mathbb{F}_p$ pentru a aplica teoria curbelor eliptice la criptografie.

Definiţia 2.20. *Fie $\mathbb{F}_p$ un corp comutativ, unde p este număr prim, cu $p \geq 3$. Fie $a, b \in \mathbb{F}_p$ două elemente aparținând de corpul $\mathbb{F}_p$ și $f(X) = X^3 + aX + b$ un polinom cu coeficienți în $\mathbb{F}_p$. Acest polinom definește o curbă eliptică peste corpul $\mathbb{F}_p$:*

$$E(\mathbb{F}_p) = \{(X, Y) \in \mathbb{F}_p^2 : Y^2 = f(X)\} \cup \{O\}$$
$$cu\ \Delta_E = 4a^3 + 27b^2 \neq 0$$

Remarca 2.21. *Momentan numărul prim p va fi $p \geq 3$. Curbelor eliptice peste $\mathbb{F}_2$ și peste $\mathbb{F}_{2^k}$ sunt importante, dar sunt de o complexitate mai ridicată.*

Datele din exemplu au fost preluate din [2].

Exemplul 2.22. *Fie curbă eliptică E peste* $\mathbb{F}_5$*:*

$$E : Y^2 = X^3 + 1 \,(mod\, 5) \tag{6}$$

O metodă de a determina punctele curbei eliptice E($\mathbb{F}_5$*) este de a da toate valorile lui X:* $0, 1, 2, 3, 4$*:*

$$f(0) = 0 + 1 = 1$$

$$f(1) = 1 + 1 = 2$$

$$f(2) = 8 + 1 = 3 + 1 = 4$$

$$f(3) = 27 + 1 = 2 + 1 = 3$$

$$f(4) = 64 + 1 = 4 + 1 = 5 = 0$$

Și să verificăm îm ecuația curbei care rezultate sunt resturi pătratice:

$$0^2 \equiv 0 \, mod \, 5$$

$$1^2 \equiv 4^2 \equiv 1 \, mod \, 5$$

$$2^2 \equiv 3^2 = 4 \, mod \, 5$$

Observăm că doar 0, 1 și 4 sunt resturi pătratice, deci spre exemplu pentru X = 0, $Y^2 = f(X) = 1$*, ceea ce înseamnă că y poate fi* $\pm 1 \,(mod\, 5)$*, adică 1 sau 4, deci rezultă punctele (0, 1) și (0, 4) în E(*$\mathbb{F}_5$*).*

Analog determinăm restul punctelor:

$$E(\mathbb{F}_5) = \big\{(0,1),(0,4),(2,2),(2,3),(4,0),O\big\}$$

Astfel, cardinalul mulțimii E($\mathbb{F}_5$) este 6.

2.4 Adunarea punctelor pe Curbe Eliptice peste Câmpuri Finite

Fie o curbă eliptică E peste $\mathbb{F}_p$:

$$E : Y^2 = X^3 + aX + b \,(mod\, p)$$

și punctele $P(x_1, y_1)$ și $Q(x_2, y_2)$ de pe E($\mathbb{F}_p$) și punctul $R(x_3, y_3)$ rezultatul adunării dintre P și Q. Algoritmul de adunare a punctelor P și Q este același ca la Teorema 2.19, doar că operațiile vor fi modulo p, nu în $\mathbb{R}$. Observăm că operațiile folosite sunt adunarea, scăderea, înmulțirea și împărțirea asupra coordonatelor punctelor și coeficienților lui E. Și cum operațiile folosite sunt închise cu $\mathbb{F}_p$, înseamnă că și rezultatul va fi tot în $\mathbb{F}_p$.

Următorul paragraf este preluat și adaptat din [1].

Teorema 2.23. *Fie o curbă eliptică E peste $\mathbb{F}_p$:*

$$E : Y^2 = X^3 + aX + b \,(mod\, p)$$

și punctele $P(x_1, y_1)$ și $Q(x_2, y_2)$ de pe E($\mathbb{F}_p$).

(a) Algoritmul de adunare a punctelor pe o curbă eliptică (Teorema 2.19) aplicat pe punctele P și Q rezultă într-un punct în E($\mathbb{F}_p$). Notăm acest punct cu P + Q.

(b) Această lege de adunare pe E($\mathbb{F}_p$) satisface toate proprietățile enumerate în Teorema 2.18. Cu alte cuvinte, E($\mathbb{F}_p$) cu legea de adunare formează un grup finit.

Exemplul 2.24. *Considerăm aceeași curbă eliptică E în $\mathbb{F}_5$ de la* (6) *și fie punctele $P(0,1)$ și $Q(2,3)$ de pe E($\mathbb{F}_5$). Folosind algoritmul de adunare a punctelor pe o curbă eliptică (Teorema 2.19) realizăm P + Q, începând cu calculul pănții dreptei:*

$$\begin{aligned} m &= \frac{y_2 - y_1}{x_2 - x_1} \\ &= \frac{2-0}{3-1} \\ &= \frac{2}{2} = 1 \end{aligned}$$

În continuare calculăm ν:

$$\begin{aligned} \nu &= y_1 - mx_1 \\ &= 1 - (1 \cdot 0) = 1 \end{aligned}$$

Ne rămâne de calulat doar rezultatul adunării:

$$\begin{aligned} x_3 &= m^2 - x_1 - x_2 \\ &= 1^2 - 0 - 2 \\ &= -1 = 4 \\ y_3 &= -(mx_3 + \nu) \\ &= -(1 \cdot 4 + 1) \\ &= -5 = 0 \end{aligned}$$

Cum calculăm în $\mathbb{F}_5$, $-1 \equiv 4 \,(mod\, 5)$ *și* $-5 \equiv 0 \,(mod\, 5)$. *Deci, rezultatul final este:*

$$P(0,1) + Q(2,3) = (4,0)$$

Analog, conform teoremei de adunare, putem aduna și $P(0,1) + P(0,1)$*:*

$$\begin{aligned} m &= \frac{3x_1^2}{2y_1} \\ &= \frac{0^2}{2 \cdot 1} = 0 \\ \nu &= y_1 - mx_1 \\ &= 1 - (0 \cdot 0) = 1 \end{aligned}$$

Și, în final:

$$\begin{aligned} x_3 &= m^2 - x_1 - x_2 \\ &= 0^2 - 0 - 0 = 0 \\ y_3 &= -(mx_3 + \nu) \\ &= -(0 \cdot 0 + 1) \\ &= -1 = 4 \end{aligned}$$

Deci, rezultatul final este:

$$P(0,1) + P(0,1) = (0,4)$$

Putem face analog toate adunările din E($\mathbb{F}_5$*) și ar rezulta:*

+	∞	(0,1)	(0,4)	(2,2)	(2,3)	(4,0)
∞	∞	(0,1)	(0,4)	(2,2)	(2,3)	(4,0)
(0,1)	(0,1)	(0,4)	∞	(2,3)	(4,0)	(2,2)
(0,4)	(0,4)	∞	(0,1)	(4,0)	(2,2)	(2,3)
(2,2)	(2,2)	(2,3)	(4,0)	(0,4)	∞	(0,1)
(2,3)	(2,3)	(4,0)	(2,2)	∞	(0,1)	(0,4)
(4,0)	(4,0)	(2,2)	(2,3)	(0,1)	(0,4)	∞

Figure 1: Tabelul de adunare pentru $E : Y^2 = X^3 + 1$ mod 5

Este evident că mulțimea punctelor din E($\mathbb{F}_p$) este finită, numărul maxim de posibilități fiind p pentru X și p pentru Y, adică p^2 aranjamente. Dar cum ecuația curbei eliptice peste un câmp finit este:

$$E : Y^2 = X^3 + aX + b \, mod \, p$$

Înseamnă că pentru fiecare Y există maxim 2 valori X care pot exista. Luând în considerare și punctul O, ajungem la $\#E(\mathbb{F}_p)$ (cardinalul grupului $E(\mathbb{F}_p)$) are cel mult $2p + 1$ puncte cu tot cu punctul O (punctul la infinit). Acest estimat este doar o margine superioară și este mult mai mare decât valoarea în practică.

Următorul paragraf este preluat și adaptat din [1].

Când introducem o valoare pentru X, există trei posibilități pentru valoarea cantității:

$$E : Y^2 = X^3 + aX + b$$

În primul caz, poate fi un rest pătratic modulo p, caz în care are două pătrate și obținem două puncte în E($\mathbb{F}_p$). Acest lucru se întâmplă în aproximativ 50% din

cazuri. În al doilea rând, poate fi un modulo p nereziduu, caz în care aruncăm X. Aceasta se întâmplă și în aproximativ 50% din timp. În al treilea rând, ar putea fi egal cu 0, caz în care obținem un punct în E($\mathbb{F}_p$), dar acest caz se întâmplă foarte rar. Astfel am putea aștepta ca numărul de puncte din $E(\mathbb{F}_p)$ să fie aproximativ:

$$\#E(\mathbb{F}_p) \approx 50\% \cdot 2p + 1 = p + 1$$

Teorema 2.25. *(Hasse) Fie E o curbă eliptică peste $\mathbb{F}_p$, atunci*

$$\#E(\mathbb{F}_p) = p + 1 - t_p \; cu \; |t_p| \leq 2\sqrt{p}$$

Definiţia 2.26. *Cantitatea:*

$$t_p = p + 1 - \#E(\mathbb{F}_p)$$

din Teorema 2.25 se numește urma lui Frobenius pentru E/($\mathbb{F}_p$), t_p apare ca urma unei anumite matrice 2 pe 2 care acționează ca o transformare liniară pe un anumit spațiu vectorial bidimensional asociat cu E($\mathbb{F}_p$).

Următorul exemplu este preluat și adaptat din [1].

Exemplul 2.27. *Fie E o curbă eliptică:*

$$E : Y^2 = X^3 + 4X + 6$$

Ne putem gândi la E ca la o curbă eliptică peste $\mathbb{F}_p$ pentru diferite câmpuri finite $\mathbb{F}_p$ și numărăm cardinalul din E($\mathbb{F}_p$). Figura 2 listează rezultatele pentru primele

câteva numere prime, împreună cu valoarea lui t_p și, în scop de comparație, a valorii de $2\sqrt{p}$.

p	$\#E(\mathbb{F}_p)$	t_p	$2\sqrt{p}$
3	4	0	3.46
5	8	−2	4.47
7	11	−3	5.29
11	16	−4	6.63
13	14	0	7.21
17	15	3	8.25

Figure 2: Cardinalul si urma lui Frobenius pentru $E : Y^2 = X^3 + 4X + 6$

Următorea remarcă este inspirată din [1].

Remarca 2.28. *Teorema lui Hasse (Teorema 2.25) oferă doar o limită superioară pentru $\#E(\mathbb{F}_p)$, ci nu oferă o metodă de calcul a acesteia. În principiu, se poate realiza "brut force", adică a se înlocui fiecare valoare a lui X din intervalul $\left[0, 1, \cdots p-1\right]$ și verificat rezultatul ecuației curbei (adică Y^2) față de un tabel precalculat cu toate pătratele modulo p. Acest proces ar dura $O(p)$ (timp liniar față de numărul prim p), deci este foarte ineficient. Schoof a găsit un algoritm pentru a calcula $\#E(\mathbb{F}_p)$ în $O((logp)^6)$ (un algoritm de timp polinomial). Algoritmul lui Schoof a fost îmbunătățit și făcut practic de Elkies și Atkin, așa că acum este cunoscut ca algoritmul SEA (după inițialele celor trei).*

Acest capitol a avut ca scop sumarizarea conceptelor de bază a curbelor eliptice pentru aplicarea acestora în criptografie. Există multe articole și cărți ce explică

teoria și concepte mai avansate, câteva exemple fiind: [4], [5], [6], [7], [8].

3 Preliminarii și concepte de bază în Criptografie

3.1 Problema Logaritmului Discret (DLP)

Problema Logaritmului Discret, sau mai bine cunoscută după numele din engleză: Discrete Logarithm Problem (DLP) apare în multe probleme matematice, însă, pentru cubele eliptice apare cel mai des peste câmpuri finite $\mathbb{F}_p$ ($\mathbb{F}_p$ fiind un corp comutativ, iar p fiind un număr prim). Prima carte publicată ce abordează construirea de chei publice se bazează pe problema logaritmului discret peste câmpuri finite $\mathbb{F}_p$ și a fost realizată de Diffie și Hellman [3] (dacă aceste nume par cunoscute, acest fapt se datorează algoritmului de schimbări de chei ce le poartă numele).

Reamintim "mica" Teoremă a lui Fermat și Teorema rădăcinii primitive. Cele trei exemple legate de mica Teorema lui Fermat și Teorema rădăcinii primitive au fost preluate din [1].

Teorema 3.1. *(Mica Teoremă a lui Fermat) Fie p un număr prim si a un număr întreg, atunci*

$$a^{p-1} \equiv \begin{cases} 1 \,(mod\, p) & \textit{dacă } p \nmid a \\ 0 \,(mod\, p) & \textit{dacă } p \mid a \end{cases}$$

Exemplul 3.2. *Fie numărul prim* $p = 15485863$*, deci Teorema 3.1 ne spune că*

$$2^{15485862} \equiv 1 \,(mod\, 15485863)$$

Astfel, fără a face niciun calcul putem să determinăm că numărul $2^{15485862} - 1$*, ce are aproximativ 4661709 de cifre (pentru determinarea nuărului de cifre am folosit acest calculator), este multiplu al numărului 15485863.*

Remarca 3.3. *(a) Din exemplul anterior observăm că oricât de mare ar fi un număr prim p, putem să determinăm un multiplu al său, acesta fiind:*

$$2^p - 1$$

(b) Acesta remarcă este preluată din [1]. Folosind mica Teoremă a lui Fermat și algoritmul de ridicat rapid la putere, putem să determinăm eficient inverselele modulo-ului p, adică

$$a^{p-2} \equiv a^{-1} \, (mod \, p)$$

Putem demonstra a doua remarcă înmulțind de ambele părți cu a și obținem mica Teoremă a lui fermat $a^{p-1} \equiv 1 \, (mod \, p)$.

Exemplul 3.4. *Fie numărul prim* $p = 17449$ *și numărul 7814. Putem calcula inversa lui 7814 modulo 17449 în doua moduri.*

Primul este să folosim remarca anterioară:

$$7814^{17447} \equiv 7814^{-1} \equiv 1284 \, (mod \, 17449)$$

A doua este să folosim algoritmul Euclidian extins pentru a rezolva

$$7814u + 17449v = 1$$

Soluția fiind (u, v) *= (1284, -575), deci* $7814^{-1} \equiv 1284 \, (mod \, 17449)$.

Teorema 3.5. *(Teorema rădăcinii primitive) Fie p un număr prim, există un element*

$g \in \mathbb{F}_p^*$, astfel încăt puterile lui g generează fiecare element al lui $\mathbb{F}_p^*$.

$$\mathbb{F}_p^* = \left\{1, g, g^2, ..., g^{p-2}\right\}$$

Elementele cu această proprietate se denumesc rădăcinini primitive ale lui $\mathbb{F}_p$ sau generatoare ale $\mathbb{F}_p$. Ele sunt elemente ale mulțimii finite $\mathbb{F}_p^*$, având ordinul $p-1$.

Exemplul 3.6. *Câmpul finit $\mathbb{F}_{11}$ îl are pe 2 ca generator, deoarece în $\mathbb{F}_{11}$*

$$2^0 = 1 \;\; 2^1 = 2 \;\; 2^2 = 4 \;\; 2^3 = 8$$
$$2^4 = 5 \;\; 2^5 = 10 \;\; 2^6 = 9 \;\; 2^7 = 7$$
$$2^8 = 3 \;\; 2^9 = 6$$

Deoarece toate elementele nenule ale mulțimii $\mathbb{F}_{11}$ au fost generate din puteri ale lui 2. Însă câmpul finit $\mathbb{F}_{17}$ nu îl are pe 2 ca generator, deoarece în $\mathbb{F}_{17}$

$$2^0 = 1 \;\; 2^1 = 2 \;\; 2^2 = 4 \;\; 2^3 = 8$$
$$2^4 = 16 \;\; 2^5 = 15 \;\; 2^6 = 13 \;\; 2^7 = 9$$
$$2^8 = 1$$

Observăm că $2^0 = 2^8 = 1$, deci nu putem crea toate elementele nenule ale mulțimii $\mathbb{F}_{17}$.

Demonstrațiile acestor teoreme (Teorema lui Fermat și Teorema rădăcinii primitive) sunt mai complexe și sunt prezentate și detaliate în amănunt în cărtea [9].

Definiţia 3.7. *(Problema Logaritmului Discret) Fie g o rădăcină primă a $\mathbb{F}_p$ și $h \in \mathbb{F}_p^*$. Problema Logaritmului Discret este problema identificării exponentului x astfel încât*

$$g^x \equiv h \,(mod\, p)$$

Numărul x se numește logaritmul discret al lui h cu baza în g și se notează $log_g(h)$.

Aceste paragraf a fost preluat și adaptat din [1].

Remarca 3.8. *(a) Fie g o rădăcină primă a $\mathbb{F}_p$, cu p număr prim și $h \in \mathbb{F}_p^*$, problema logaritmului discret presupune identificarea numărului x pentru ca $g^x \equiv h \,(mod\, p)$. Conform micii Teoreme a lui Fermat (Teorema 3.1) avem $g^{p-1} \equiv 1 \,(mod\, p)$, ceea ce înseamnă ca dacă înmulțim g^x cu g ridicat la un multiplu de (p - 1) rezutatul va fi tot h. Mai exact, dacă x este soluția căutată, atunci și $x + k(p-1)$ cu $k \in \mathbb{Z}^*$ este o soluție. Adică*

$$\begin{aligned} g^{x+k(p-1)} &= g^x \cdot g^{k\cdot(p-1)} \\ &= g^x \cdot (g^{(p-1)})^k \end{aligned}$$

$$g^x \cdot (g^{(p-1)})^k \equiv h \cdot 1^k \equiv h \,(mod\, p)\; pentru\; orice\; k \in \mathbb{Z}^*$$

De aceea precizăm că ne referim la soluția logaritmului discret ca fiind x-ul din intervalul [0, ... p - 2].

(b) Este rezonabil să ne referim la log_g ca fiind un „logaritm", deoarece traduce înmulțirea în adunare în același mod ca și funcția normală de logaritm.

Definiţia 3.9. *Fie G un grup a cărei lege de compoziție o notăm ca fiind $\star$. Problema Logaritmului Discret pentru grupul G este problema identificării, pentru orice două elemente h și g cu $h, g \in G$, numărul întreg x astfel încât*

$$\underbrace{g \star g \star g \star ... \star g}_{x \text{ times}} = h$$

3.2 Schimbul de chei Diffie–Hellman

În istoria comunicațiilor secrete, crearea criptografiei cu cheie publică de către Diffie și Hellman în 1976 și urmat de criptosistemul cu chei publice RSA (după inițialele autorilor) realizat de Rivest, Shamir și Adleman în 1978, sunt momente definitorii. Semnificația criptosistemelor cu chei publice și a protocoalelor de semnătură digitală pe care le suportă nu poate fi măsurată în era curentă a computerelor și a internetului.

Unul din obiectivele principale al criptografiei (cu cheia publică) este de a permite ca două persoane să facă schimb de informații confidențiale, chiar dacă nu s-au întâlnit niciodată și pot comunica doar prin intermediul unui canal care este monitorizat de un adversar. Adică de a putea comunica pe un canal nesigur, fără necesitatea întâlnirii anterioare.

Înainte vom defini câteva notații pe care le fom folosi de acum înainte în cadrul acestei lucrări. Persoanele ce doresc să communice între ele le vom denumi Alice (va fi notată cu A) și Bob (va fi notat cu B). iar adversarul, cel ce dorește să determine mesajul trimis o vom numi Eve (va fi notată cu E).

Codurile și cifrurile până de curând s-au bazat pe premisa că părțile care încercau să comunice (Bob și Alice) au împărtășit o cheie secretă pe care inamicul lor, să-i

spunem Eve, nu o știe. Bob și-ar cripta mesajul folosind cheia secretă și Alice l-ar decripta folosind aceeași cheie secretă, iar Eve nu putea să realizeze decriptarea mesajului, deorece nu are acces la cheia secretă. Totuși există un mare dezavantaj la criptosistemele cu cehie privată, și acela este că Alice și Bob trebuie să stabilească cheia secretă a priori conversației.

Acesta este și avantajul principal al criptografiei cu cheie publică, Alice și Bob pot comunica pe un canal nesigur, chiar dacă nu au avut contact cirect înainte. Aceste criptosisteme se bazează pe probleme grele din matematică, precum Problema Logaritmului Discret studiată anterior, pentru a asigura securitatea comunicării. Mai precis, se bazează pe probleme ce este foarte complicat de rezolvat fără nicio informații suplimentare, dar care se pot rezolva ușor cu date suplimentare.

Diffie și Hellman au folosit dificultatea Problemei Logaritmului Discret peste $\mathbb{F}_p^*$ a realiza schimbul de chei între cei ce comunică.

Schimbul de chei Diffie-Hellman este un protocol criptografic care permite celor două părți participante să stabilească o cheie secretă partajată pe un canal de comunicare nesigur. A fost introdus de Whitfield Diffie și Martin Hellman în 1976 și este utilizat pe scară largă pentru stabilirea securizată a cheilor în diferite sisteme criptografice. Vom determina importanța existenței acestui algoritm în capitolele viitoare în cadrul criptografiei bazate pe curbe eliptice.

Acesta este algoritmul ce se aplică pentru schimbul de chei Diffie-Hellman:

(1) Configurare: cele două părți ce comunicare, Alice și Bob, convin asupra anumitor parametri:

- un număr prim foarte mare pe care o să-l notăm cu p

- un număr întreg nenul g modulo p

  notă: numărul g ar trebui să fie ales astfel încât ordinul său în $\mathbb{F}_p^*$ să fie un număr prim mare

  notă: cum comunicarea se realizează pe un canal neprivat, Eve are acces la p și g

(2) Alegerea numerelor secrete:

- Alice alege un număr întreg secret a pe care nu-l împărtașește cu nimeni și calculează

$$A \equiv g^a \ (mod\, p)$$

- Bob alege un număr întreg secret b pe care nu-l împărtașește cu nimeni și calculează

$$B \equiv g^b \ (mod\, p)$$

(3) Schimbul de chei secrete: Alice îi trimite A lui Bob si Bob îi trimite B lui Alice pe canalul neprivat

- Alice își folosește numărul secret și calculează

$$A' \equiv B^a \ (mod\, p)$$

- Bob își folosește numărul secret și calculează

$$B' \equiv A^b \ (mod\, p)$$

notă: cum comunicarea se realizează pe un canal neprivat, Eve are acces la A și B

(4) Cheie secretă comună rezultată: valorile pe care le calculează sunt egale și reprezintă cheia comună

$$A' \equiv B^a \equiv (g^b)^a \equiv g^{ab} \equiv (g^a)^b \equiv A^b \equiv B' \, (mod \, p)$$

Schimbul de chei Diffie-Hellman este sumarizat în Figura 3.

Public Parameter Creation	
A trusted party chooses and publishes a (large) prime p and an integer g having large prime order in $\mathbb{F}_p^*$.	
Private Computations	
Alice	**Bob**
Choose a secret integer a.	Choose a secret integer b.
Compute $A \equiv g^a \pmod{p}$.	Compute $B \equiv g^b \pmod{p}$.
Public Exchange of Values	
Alice sends A to Bob $\longrightarrow$	A
B $\longleftarrow$	Bob sends B to Alice
Further Private Computations	
Alice	**Bob**
Compute the number $B^a \pmod{p}$.	Compute the number $A^b \pmod{p}$.
The shared secret value is $B^a \equiv (g^b)^a \equiv g^{ab} \equiv (g^a)^b \equiv A^b \pmod{p}$.	

Figure 3: Schimbul de chei Diffie-Hellman

Datele din exemplul următor au fost preluate din [1].

Exemplul 3.10. *Vom urma pașii din algoritmul prezentat anterior.*

Pasul 1, Alice și Bob stabilesc numărul $p = 941$ și rădăcina primitivă $g = 627$.

Pasul 2, Alice alege numărul întreg secret $a = 347$ și calculează

$$A = 390 \equiv 627^{347} \ (mod\, 941)$$

Analog, Bob alege numărul întreg secret $b = 781$ și calculează

$$B = 691 \equiv 627^{781} \ (mod\, 941)$$

Pasul 3, Alice îi trimite 390 (A) lui Bob și Bob îi trimite 691 (B) lui Alice pe canalul nesecurizat.

Alice își folosește numărul secret și calculează

$$A' = 470 \equiv 691^{347} \ (mod\, 941)$$

Bob își folosește numărul secret și calculează

$$B' = 470 \equiv 390^{781} \ (mod\, 941)$$

Pasul 4, Alice și Bob au obținut cheia secretă comună

$$470 \equiv 627^{390 \cdot 781} \equiv A^b \equiv B^a \ (mod\, 941)$$

Eve are acces la următoarele date: 941(f), 627(g), 390(A) și 691(B). Ceea ce înseamnă ca dacă Eve dorește să determine cheia secretă comună a lui Alice și Bob, aceasta trebuie să rezolve una din cele două congruențe pentru a determina numărul

secret a al lui Alice sau b al lui Bob:

$$627^a \equiv 390 \ (mod\, 941)$$

$$627^b \equiv 691 \ (mod\, 941)$$

Observăm că ecuațiile anterioare reprezintă Problema Logaritmului Discret (în Definiția 3.7). Pentru a găsi rezolvarea, Eve trebuie să dea "brute force", încercând toate puterile lui 627 modulo 941 pentru a găsi una din cele două congruențe. Ea nu ar avea problema pe exemplul oferit, deoarece numerele sunt mici, însă în practică, în 2008 se recomanda ca p să aibă mai mult 1000 de cifre în compoziția sa și g să aibă ordin un număr prim aproximativ jumătate din p.

Astfel, Problema Logaritmului Discret oferă securitate schimbului de chei Diffie-Hellman.

Dacă Eve nu poate rezolva Problema Logaritmului Discret, ar părea că Alice și Bob sunt în siguranță, dar acest lucru nu este neapărat adevărat. Rezolvarea Problemei Logaritmului Discret este o modalitate de a determina valoarea comună a lui Alice și Bob, dar aceasta nu este problema specifică pe care Eve vrea să o rezolve, aceasta încercâd să determine valoarea $g^{ab} \ (mod\, p)$. Securitate cheii comune transmise între Alice și Bob este dată de dificultatea cu care se rezolvă următoarea problemă, ce este potențial mai ușoară.

Definiţia 3.11. *(Problema Diffie-Hellman) Fie p un număr prim și g un număr întreg. Problema Diffie-Hellman, sau Diffie–Hellman Problem (DHP) în engleză, este problema determinării valorii $g^{ab} \ (mod\, p)$ cunoscând $g^a \ (mod\, p)$ și $g^b \ (mod\, p)$.*

Remarca 3.12. *Presupunem că există un algoritm eficient care să rezolve Problema Diffie-Hellman, momentan nu se știe dacă se poate folosi acest algoritm pentru a*

rezolva eficient Problema Logaritmului Discret.

3.3 Criptosistemul cu cheie publică ElGamal

Chiar dacă din punct de vedere istoric, RSA a fost primul criptosistem cu cheie publică, dezvoltarea naturală a unui criptosistem în urma lucrării realizate de Diffie și Hellman (Lucrarea [3]) este un sistem descris de Taher ElGamal în 1985 în [10]. Algoritmul ElGamal pentru criptarea de chei publice se bazează pe Problema Logaritmului Discret și se aseamănă cu schimbul de chei Diffie-Hellman prezentat în subcapitolul anterior. În continuare vom detalia criptosistemul cu cheie publică El Gamal ce se bazează pe Problema Logaritmului Discret pe $\mathbb{F}_p^*$.

Acesta este algoritmul dacă Bob dorește să-i trimită un mesaj lui Alice:

(1) Configurare: se stabilesc parametrii publici:

- un număr prim foarte mare pe care o să-l notăm cu p
- un număr întreg nenul g modulo p

  notă: numărul g ar trebui să fie ales astfel încât ordinul său în $\mathbb{F}_p^*$ să fie un număr prim mare

  notă: cum comunicarea se realizează pe un canal neprivat, Eve are acces la p și g

(2) Crearea cheii secrete:

- Alice alege o cheie secretă a din intervalul $[1, 2, ..., p-1]$ pe care nu-l împărtașește cu nimeni

- Alice calculează cheia publică A

$$A = g^a \ (mod\, p)$$

- Alice își publică cheia publică

(3) Criptarea:

- Bob alege mesajul m pe care dorește să-l trmită
- Bob alege o cheie aleatore temporală k
- Bob folosește cheia publică a lui Alice pentru a calcula

$$c_1 = g^k \ (mod\, p)$$
$$c_2 = mA^k \ (mod\, p)$$

- Bob îi trimtie mesajul criptat (c_1, c_2) lui Alice

  notă: cum comunicarea se realizează pe un canal neprivat, Eve are acces la (c_1, c_2)

(4) Decriptarea

- Alice calculează

$$(c_1^a)^{-1} \cdot c_2 \ (mod\, p)$$

- rezultatul obținut este m

Algoritmul ElGamal pentru creare de chei, criptare și decriptare este sumarizat în Figura 4.

Public Parameter Creation	
A trusted party chooses and publishes a large prime p and an element g modulo p of large (prime) order.	
Alice	**Bob**
Key Creation	
Chooses private key $1 \leq a \leq p-1$. Computes $A = g^a \pmod{p}$. Publishes the public key A.	
Encryption	
	Chooses plaintext m. Chooses random ephemeral key k. Uses Alice's public key A to compute $c_1 = g^k \pmod{p}$ and $c_2 = mA^k \pmod{p}$. Sends ciphertext (c_1, c_2) to Alice.
Decryption	
Compute $(c_1^a)^{-1} \cdot c_2 \pmod{p}$. This quantity is equal to m.	

Figure 4: Algoritmul ElGamal pentru creare de chei, criptare și decriptare

Arătăm că rezultatul ecuației $(c_1^a)^{-1} \cdot c_2 \ (mod\ p)$ obținut de Alice chiar este mesajul m

$$\begin{aligned}(c_1^a)^{-1} \cdot c_2 &\equiv (g^{ak})^{-1} \cdot (mA^k)\ (mod\, p)\\ &\equiv (g^{ak})^{-1} \cdot (m(g^a)^k)\ (mod\, p)\\ &\equiv (g^{ak})^{-1} \cdot g^{ak} \cdot m\ (mod\, p)\\ &\equiv m\ (mod\, p)\end{aligned}$$

Datele din exemplul următor au fost preluate din [1].

Exemplul 3.13. *Vom urma pașii din algoritmul prezentat anterior.*

Pasul 1, se stabilesc $p = 467$ *și rădăcina primitivă* $g = 2$*.*

Pasul 2, Alice alege numărul întreg secret $a = 153$ *și calculează*

$$A = 224 \equiv 2^{153} \, (mod \, 467)$$

Alice anunță cheia publică A

Pasul 3, Bob alege mesajul $m = 331$*, cheia aleatoare temporală* $k = 197$ *și criptează mesajul*

$$c_1 = 87 \equiv 2^{197} \, (mod \, 467)$$
$$c_2 = 57 \equiv 331 \cdot 224^{197} \, (mod \, 467)$$

Bob îi trimite lui Alice mesajul criptat $(c_1, c_2) = (87, 57)$*.*

Pasul 4, Alice decriptează mesajul primit de la Bob

$$\begin{aligned}(c_1^a)^{-1} \cdot c_2 &\equiv (87^{153})^{-1} \cdot 57 \, (mod \, 467) \\ &\equiv 367^{-1} \cdot 57 \, (mod \, 467) \\ &\equiv 14 \cdot 57 \equiv 331 \, (mod \, 467)\end{aligned}$$

Eve cunoaște următoarele date: numărul prim p, rădăcina primitivă g, cheia publică A și mesajul criptat (c_1, c_2). Dacă Eve dorește să afle mesajul decriptat m pe care Bob i l-a trimis lui Alice, atunci Eve trebuie să rezolve $A \equiv g^a \, (mod \, p)$. Observăm că Eve trebuie să rezolve Problema Logaritmului Discret ca să determine valorea mesajului transmis .

Remarca 3.14. *În criptosistemul de chei publice ElGamal, mesajul inițial* m *pe care Bob dorește să-l trimită lui Alice este un număr din intervalul* $[2, 3, ..., p - 1]$. *Numerele din componența mesajului criptat* c_1 *și* c_2 *sunt tot din intervalul* $[2, 3, ..., p - 1]$ *și de o lungime asemănătoare cu* m. *Astfel, pentru fiecare mesaj pe care Bob dorește să-l trimită lui Alice lungimea textului criptat va fi aproximativ de două ori mai mare. De aceea, spunem că ElGamal are o expansiune a mesajului inițial de* $2\ la\ 1$.

Legat de securitatea criptosistemului ElGamal, am vrea ca acesta să fie cel puțin la fel de greu de atacat de către Eve ca Problema Diffie-Hellman (Problema 3.11). Adică, mai exact am vrea să demonstrăm că dacă Eve poate sparge criposistemul ElGamal, aceasta poate rezolva Problema Diffie-Hellman.

Următoarea propoziție și demonstrație au fost preluate și adaptate din [1].

Propoziţia 3.15. *Fie un număr prim* p *și o rădăcină* g *pe care le folosim pentru crpitarea ElGamal. Să presupunem că Eve are acces la un oracol care decriptează ElGamal texte cifrate criptate arbitrare folosind chei publice arbitrare ElGamal. Atunci ea poate folosi oracolul pentru a rezolva Problema Diffie–Hellman (Problema 3.11).*

Demonstraţie. În loc să oferim o demonstrație clasică, vom vorbi mai mult și vom explica cum s-ar putea aborda problema utilizării unui oracol ElGamal pentru a rezolva Problema Diffie–Hellman. Reamintim că în Problema Diffie–Hellman, Evei i se dau cele două valori

$$A \equiv g^a \ (mod\, p)$$

$$B \equiv g^b \ (mod\, p)$$

Și i se cere să determine valoarea $g^{ab}\ (mod\ p)$. Eve cunoaște ambele valori ale lui A și B, dar nu cunoaște niciuna dintre valorile valorile a și b.

Presupunem că Eve poate consulta un oracol ElGamal. Asta înseamnă că Eve poate trimite oracolului un număr prim p, o bază g, o cheie publică A și un text cifrat $(c1, c2)$. Oracolul revine răspunde cu m, adică returnează valoarea

$$(c_1^a)^{-1} \cdot c_2\ (mod\ p)$$

Dacă Eve alege să-i dea oracolului inputul $c_1 = B = g^b$ și $c_2 = 1$, atunci oracolul o să returneze $(g^{ab})^{-1}\ (mod\ p)$, din care se poate determina din inversă $(g^{ab})\ (mod\ p)$, rezolvând Problema Diffie-Hellman.

Dar în cazul în care oracolul este suficient de inteligent pentru a ști că nu ar trebui să decripteze niciodată texte cifrate care au $c_2 = 1$, Eve poate încă păcăli oracolul trimițându-i texte cifrate aleatorii, după cum urmează. Ea alege o valoare arbitrară pentru c_2 și îi dă oracolului cheia publică A și textul cifrat (B, c_2). Oracolul îi returnează presupusul text clar m care satisface

$$\begin{aligned} m &\equiv (c_1^a)^{-1} \cdot c_2\ (mod\ p) \\ &\equiv (B^a)^{-1} \cdot c_2\ (mod\ p) \\ &\equiv (g^{ab})^{-1} \cdot c_2\ (mod\ p) \end{aligned}$$

După răspunsul oracolului cu valoarea m, Eve calzulează

$$m^{-1} \cdot c_2 \equiv g^{ab}\ (mod\ p)$$

pentru a găsi valoarea lui $g^{ab}\ (mod\ p)$. Este de remarcat faptul că, deși, cu ajutorul oracolului, Eve a calculat $g^{ab}\ (mod\ p)$, a făcut-o fără cunoașterea valorii lui a sau b, așa că a rezolvat doar Problema Diffie-Hellman, nu și Problema logaritmului discret. □

Remarca 3.16. *Un atac în care Eve are acces la un oracol care decriptează texte cifrate arbitrare sunt cunoscute ca un "chosen ciphertext attack". Propoziția precedentă arată că sistemul ElGamal este sigur împotriva unui astfel de atac.*

3.4 Criptosistemul cu cheie publică RSA

4 Criptografia pe Curbe Eliptice

4.1 Problema Logaritmului Discret pe Curbe Eliptice (ECDLP)

4.2 Schimbul de chei Diffie–Hellman pe Curbe Eliptice

Urmează să aplicăm curbe eliptice în criptografie. Începem cu schimbul de chei Diffie-Hellman, pentru care cam tot ce trebuie să facem este să schimbăm Problema Logaritmului Discret peste câmpul finit $\mathbb{F}_p$ cu Problema Logaritmului Discret pe curba eliptică E($\mathbb{F}_p$).

Vom trece prin aceleași etape ca la schimbul de chei Diffie-Hellman normal.

Acesta este algoritmul ce se aplică pentru schimbul de chei Diffie-Hellman pe curbe eliptice:

(1) Configurare: cele două părți ce comunicare, Alice și Bob, convin asupra anumitor parametri:

- un număr prim foarte mare pe care o să-l notăm cu p
- o curbă eliptică E peste $\mathbb{F}_p$
- un punct $P \in \mathbb{F}_p$

notă: cum comunicarea se realizează pe un canal neprivat, Eve are acces la p, E și P

(2) Alegerea numerelor secrete:

- Alice alege un număr întreg secret n_A pe care nu-l împărtașește cu nimeni și calculează

$$Q_A = n_A P$$

- Bob alege un număr întreg secret n_B pe care nu-l împărtașește cu nimeni și calculează

$$Q_B = n_B P$$

(3) Schimbul de chei secrete: Alice îi trimite Q_A lui Bob si Bob îi trimite Q_B lui Alice pe canalul neprivat

- Alice își folosește numărul secret și calculează

$$Q'_A = n_A Q_B$$

- Bob își folosește numărul secret și calculează

$$Q'_B = n_B Q_A$$

notă: cum comunicarea se realizează pe un canal neprivat, Eve are acces la Q_A și Q_B

(4) Cheie secretă comună rezultată: valorile pe care le calculează sunt egale și reprezintă cheia comună

$$Q'_A = n_A Q_B = n_A(n_B P) = n_B(n_A P) = n_B Q_A = Q'_B$$

Schimbul de chei Diffie-Hellman pe curbe eliptice este sumarizat în Figura 5.

Public Parameter Creation	
A trusted party chooses and publishes a (large) prime p, an elliptic curve E over $\mathbb{F}_p$, and a point P in $E(\mathbb{F}_p)$.	
Private Computations	
Alice	**Bob**
Chooses a secret integer n_A. Computes the point $Q_A = n_A P$.	Chooses a secret integer n_B. Computes the point $Q_B = n_B P$.
Public Exchange of Values	
Alice sends Q_A to Bob $\longrightarrow$	Q_A
Q_B $\longleftarrow$	Bob sends Q_B to Alice
Further Private Computations	
Alice	**Bob**
Computes the point $n_A Q_B$.	Computes the point $n_B Q_A$.
The shared secret value is $n_A Q_B = n_A(n_B P) = n_B(n_A P) = n_B Q_A$.	

Figure 5: Schimbul de chei Diffie-Hellman pe curbe eliptice

Datele din exemplul următor au fost preluate din [1].

Exemplul 4.1. *Vom urma pașii din algoritmul prezentat anterior. Pasul 1, Alice și Bob stabilesc numărul* $p = 3851$ *și curba eliptică E și punctul P*

$$E : Y^2 = X^3 + 324X + 1287$$

$$P = (920, 303) \in E(\mathbb{F}_{3851})$$

Pasul 2, Alice alege numărul întreg secret $n_A = 1194$ *și calculează*

$$Q_A = 1194P = (2067, 2178) \in E(\mathbb{F}_{3851})$$

Analog, Bob alege numărul întreg secret $b = 1759$ *și calculează*

$$Q_A = 1759P = (3684, 3125) \in E(\mathbb{F}_{3851})$$

Pasul 3, Alice îi trimite $(2067, 2178)$ *(*Q_A*) lui Bob și Bob îi trimite* $(3684, 3125)$ *(*Q_B*) lui Alice pe canalul nesecurizat.*

Alice își folosește numărul secret și calculează

$$Q'_A = 1194Q_A = (3347, 1242) \in E(\mathbb{F}_{3851})$$

Bob își folosește numărul secret și calculează

$$Q'_B = 1759Q_B = (3347, 1242) \in E(\mathbb{F}_{3851})$$

Pasul 4, Alice și Bob au obținut cheia secretă comună

$$(3347, 1242) = n_A n_B P = Q'_A = Q'_B$$

Punctul secret comun este $(3347, 1242)$, dar după cum va fi explicat în Remarca 4.3, suntem interesați doar de componenta x a punctului, adică cheia secretă comună va fi considerată numărul 3347.

Eve are acces la următoarele date: numărul prim p, curba eliptică E, punctul de pe curbă P și valorile Q_A și Q_B. Ceea ce înseamnă ca dacă Eve dorește să determine cheia secretă comună a lui Alice și Bob, aceasta trebuie sa rezolve una

din cele două Probleme ale Logaritmului Discret pe Curbe Eliptice

$$Q_A = n_A P$$

$$Q_B = n_B P$$

Ca la Problema Loaritmului Discret, Eve poate rezolva analogul Problemei Diffie-Hellman (Definiția 3.11) adaptată pentru curbe eliptice.

Definiţia 4.2. *(Problema Diffie-Hellman pe Curbe Eliptice) Fie $E(\mathbb{F}_p)$ o curbă eliptică peste un câmp finit și fie punctul $P \in E(\mathbb{F}_p)$. Problema Diffie-Hellman pe Curbe Eliptice este problema determinării valorii $n_1 n_2 P$ cunoscând valorile $n_1 P$ și $n_2 P$.*

Urmatoarea remarcă a fost preluată și adaptată din [1]

Remarca 4.3. *Schimbul de chei Diffie–Hellman pe curbe eliptice necesită ca Alice și Bob să schimbe puncte pe o curbă eliptică. Un punct $Q \in E(\mathbb{F}_p)$ este format din două coordonate $Q = (x_Q, y_Q)$, unde x_Q și y_Q sunt elemente ale câmpului finit $(\mathbb{F}_p)$, așa că pare că Alice trebuie să-i trimită lui Bob două numere în $(\mathbb{F}_p)$. Cu toate acestea, cele două numere modulo p nu conțin la fel de multe informații ca două numere arbitrare, deoarece sunt legate prin formula*

$$E : y_Q^2 = x_Q^3 + a x_Q + b \, (mod \, p)$$

A se nota că Eva cunoaște A și B, deci dacă poate ghici valoarea corectă a lui x_Q, atunci există doar două valori posibile pentru y_Q, iar în practică nu este greu să calculeze cele două valori ale lui y_Q.

Prin urmare, există puține motive pentru ca Alice să trimită ambele coordonate ale Q_A lui Bob, deoarece coordonata y conține puține informații suplimentare. În schimb, ea îi trimite lui Bob doar coordonatele x a puntului Q_A. Bob calculează apoi și folosește unul dintre cele două coordonate y posibile. Dacă se întâmplă să aleagă y „corect", atunci el folosește Q_A, iar dacă alege y „incorect" (care este negativul lui y corect), atunci el folosește -Q_A. În orice caz, Bob ajunge să calculeze unul dintre valorile

$$\pm n_B Q_A = \pm(n_A n_B)P$$

În mod similar, Alice ajunge să calculeze unul dintre $\pm(n_A n_B)P$. Apoi Alice și Bob utilizează coordonatele x ca valoare secretă comună, deoarece acea coordonată x este la fel indiferent de ce y folosesc.

4.3 Criptosistemul ElGamal pe curbe eliptice

4.4 Criptosistemul RSA cu curbe eliptice (ECRSA)

5 Aplicația suport

5.1 Flask

6 Rezultate

Pe înmulțirea pe curbe elitpice peste câmpuri finite nu contează componenta y a punctului ce este înmulțit, rezultatul va avea aceeași componentă x ca înmulțirea nealterată.

Spre exemplu, fie curba eliptică

$$E : Y^2 = X^3 + aX + b \, (mod \, p)$$

Și punctele $P(x_1, y_1)$ și $Q(x_1, p - y_1)$ cu $P, Q \in E(\mathbb{F}_p)$. Orice $n \in \mathbb{Z}$ am alege

$$nP = R_1(x_2, y_2)$$

$$nQ = R_2(x_2, p - y_2)$$

Bibliografie

[1] J. Hoffstein et al., *An Introduction to Mathematical Cryptography*, 1 DOI: 10.1007/978-0-387-77994-2 1, @ Springer Science+Business Media, LLC 2008.

[2] Cătălin Liviu Gherghe, *Curbe Eliptice 3*, Criptografie si Teoria Codurilor, Curs 2023.

[3] W. Diffie and M. E. Hellman. New directions in cryptography. *IEEE Trans. Information Theory*, IT-22(6):644–654, 1976.

[4] J. W. S. Cassels. *Lectures on Elliptic Curves*, volume 24 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1991.

[5] A. W. Knapp. *Elliptic Curves*, volume 40 of *Mathematical Notes*. Princeton University Press, Princeton, NJ, 1992.

[6]] S. Lang. *Elliptic Functions*, volume 112 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2nd edition, 1987. With an appendix by J. Tate.

[7] J. H. Silverman. *The Arithmetic of Elliptic Curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1986.

[8] J. H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.

[9] J. H. Silverman. *A Friendly Introduction to Number Theory*. Prentice Hall, Upper Saddle River, NJ, 3rd edition, 2006.

[10] T. ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Trans. Inform. Theory*, 31(4):469–472, 1985.

[11] L. Beznea, I. Cîmpean, Quasimartingales associated to Markov processes, Trans. Amer. Math. Soc., 370, 7761-7787 (2018).