Capitolul 10

Sisteme de criptare bazate pe curbe eliptice

Toate sistemele de criptare prezentate până în acest moment se bazează pe operaţii efectuate într-un inel multiplicativ Z_n; securitatea lor s-a redus în general la probleme matematice $\mathcal{NP}$ - complete.

În 1985, Victor Miller şi Neal Koblitz propun – independent unul de altul – o criptografie în care baza de calcul să fie mulţimea punctelor unei curbe eliptice. Se pare că sunt două motive pentru care această modalitate este exploatată cu tot mai mult succes:

- Este asigurată o eficienţă sporită a algoritmilor (din punct de vedere timp/spaţiu). Conform NSA (National Security Agency), "*criptografia pe curbe eliptice asigură o securitate sporită, precum şi performanţe superioare tehnicilor de criptare cu cheie publică cunoscute până acum.*"

  O estimare oferită de $NIST$ a mărimii cheilor (în biţi) pentru un nivel echivalent de securitate arată astfel:

Sistem simetric	*RSA*	*Sistem pe curbe eliptice*
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	521

- Oferă variante de implementare superioare pentru noi aparate matematice de calcul (cum ar fi de exemplu aplicaţiile biliniare).

Vom aborda în acest capitol o scurtă prezentare a curbelor eliptice, precum şi a principalelor direcţii de studiu referitoare la ECC (Elliptic Curve Cryptography).

10.1 Aritmetica curbelor eliptice

Pentru început, să definim noţiunea de *curbă eliptică*.

Definiţia 10.1. *O curbă eliptică E peste un corp K este definită de ecuaţia*

$$E: \quad y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{1}$$

unde $a_1, a_2, a_3, a_4, a_6 \in K$ şi $\Delta \neq 0$, unde Δ este discriminantul lui E, definit prin

$$\Delta = -d_2^2d_8 - 8d_4^3 - 27d_6^2 + 9d_2d_4d_6, \tag{2}$$

iar
$$\begin{cases} d_2 = a_1^2 + 4a_2, \\ d_4 = 2a_4 + a_1a_3, \\ d_6 = a_3^2 + 4a_6, \\ d_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4. \end{cases}$$

Dacă L este o extensie oarecare a lui K, atunci mulţimea punctelor curbei E pe L este

$$E(L) = \{(x, y) \in L \times L \mid y^2 + a_1xy + a_3y - x^3 + a_2x^2 + a_4x + a_6 = 0\} \bigcup \{\mathcal{O}\}$$

unde $\mathcal{O}$ este "*punctul de la infinit*"[1].

Elementele lui $E(L)$ se numesc *punctele L - raţionale ale curbei E.*

În general vom lucra cu un corp $K = Z_p$, unde p este un număr prim. Prin extensie, vom numi curbă eliptică peste Z_p mulţimea $(x, y) \in Z_p \times Z_p$ a soluţiilor ecuaţiei

$$y^2 + a_1xy + a_3y \equiv x^3 + a_2x^2 + a_4x + a_6 \pmod p$$

şi dintr-un punct la infinit $\mathcal{O}$.

Observaţia 10.1.

1. *Ecuaţia* (1) *este numită ecuaţie Weierstrass.*
2. *Condiţia $\Delta \neq 0$ asigură lucrul cu o curbă eliptică "netedă" (fără puncte în care curba are două sau mai multe tangente distincte).*

În funcţie de valorile caracteristicii p a corpului K, se disting următoarele cazuri:

1. $p = 2$. Apar două subcazuri:
   (a) Dacă $a_1 \neq 0$, atunci curba eliptică E poate fi adusă (prin schimbări de variabile) la forma
   $$y^2 + xy = x^3 + ax + b \tag{3}$$
   unde $a, b \in K$. O asemenea curbă se numeşte *non-supersingulară*, iar discriminantul ei este $\Delta = b$.

[1]Elementul $\mathcal{O}$ este introdus pentru a satisface forma proiectivă a ecuaţiei (1) şi pentru a permite construirea unei structuri algebrice convenabile pe $E(L)$.

(b) Dacă $a_1 = 0$, atunci ecuaţia curbei E poate fi adusă la forma

$$y^2 + cy = x^3 + ax + b \tag{4}$$

unde $a, b, c \in K$. O asemenea curbă este numită *supersingulară*, iar discriminantul ei este $\Delta = c^4$.

2. $p = 3$. Apar şi aici două subcazuri:

(a) Dacă $a_1^2 \neq -a_2$, atunci curba eliptică E se poate transforma în

$$y^2 = x^3 + ax^2 + b \tag{5}$$

cu $a, b \in K$. Curba este numită *non-supersingulară*, iar discriminantul ei este $\Delta = -a^3 b$.

(b) Dacă $a_1^2 = -a_2$, atunci E se aduce la forma

$$y^2 = x^3 + ax + b \tag{6}$$

cu $a, b \in K$. Curba este *supersingulară*, de discriminant $\Delta = -a^3$.

3. Pentru $p > 3$, curba eliptică E poate fi adusă (prin schimbări de variabile) la forma

$$y^2 = x^3 + ax + b \tag{7}$$

unde $a, b \in K$. Descriminantul ei este $\Delta = -16(4a^3 + 27b^2)$.

Marea majoritate a curbelor eliptice utilizate în protocoale criptografice sunt definite pentru cazul $p > 3$ sau (într-o măsură mai mică) pentru curbele non-supersingulare.

În continuare vom lucra cu definiţia (7) a unei curbe eliptice (cazul corpurilor de caracteristică $p > 3$).

O astfel de curbă eliptică E se poate structura ca un grup abelian finit. Legea de compoziţie (notată aditiv) este definită astfel:

Fie $P, Q \in E(L), \quad P = (x_1, y_1),\ Q = (x_2, y_2)$.

Dacă $x_2 = x_1,\ y_2 = -y_1$, atunci $P + Q = \mathcal{O}$; altfel, $P + Q = (x_3, y_3)$ unde

$$x_3 = \lambda^2 - x_1 - x_2, \quad y_3 = \lambda(x_1 - x_3) - y_1,$$

iar

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

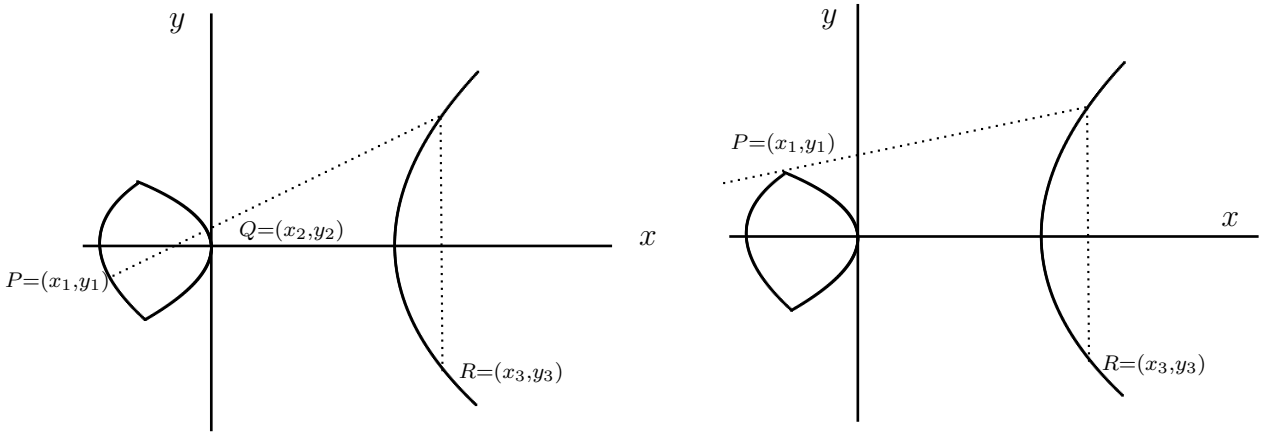
Se mai defineşte $P + \mathcal{O} = \mathcal{O} + P = P,\ \forall P \in E$.

Verificarea proprietăţilor de grup este banală. Elementul neutru este $\mathcal{O}$.

De remarcat că inversa lui (x, y) (notată $-(x, y)$) este $(x, -y)$.

Operaţia poate fi explicată mult mai sugestiv geometric.

Fie $P = (x_1, y_1)$ şi $Q = (x_2, y_2)$ două puncte distincte pe curba eliptică E. Suma $R = P + Q$ este definită astfel: linia PQ taie curba într-un al treilea punct. R este simetricul acestui punct faţă de axa xx' (figura (a)).



(a) Adunarea $P + Q = R$

(b) Dublarea: $P + P = R$

Dacă P şi Q coincid, atunci tangenta în P va tăia din nou curba eliptică E. R este simetricul acestui nou punct faţă de axa xx' (figura (b)).

Exemplul 10.1. *Fie E curba eliptică $y^2 = x^3 + x + 5$ peste Z_{19}. Să calculăm la început punctele lui E. Aceasta se face astfel: $\forall x \in Z_{11}$ se calculează $z = x^3 + x + 5 \ (mod\ 19)$; apoi se testează dacă z este rest pătratic.*

În caz afirmativ, deoarece $19 \equiv 3 \ (mod\ 4)$, există o formulă (a se vedea sistemul de criptare Rabin, Capitolul 8) care conduce direct la calculul rădăcinilor pătrate ale lui z :

$$\pm\, z^{(19+1)/4} \ (mod\ 19) \ = \pm z^5 \ (mod\ 19).$$

Rezultatele sunt strânse în tabelele următoare (toate calculele se realizează modulo 19):

a	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
a^2	0	1	4	9	16	6	17	11	7	5	5	7	11	17	6	16	9	4	1

x	x^3+x+5	y	x	x^3+x+5	y	x	x^3+x+5	y
0	5	9, 10	1	7	8, 11	2	15	–
3	16	4, 15	4	16	4, 15	5	2	–
6	18	–	7	13	–	8	12	–
9	2	–	10	8	–	11	17	6, 13
12	16	4, 15	13	11	7, 12	14	8	–
15	13	–	16	13	–	17	14	–
18	3	–						

Curba eliptică E admite deci 15 *puncte; cum ordinul grupului nu este număr prim, grupul nu este ciclic. Vom alege un element primitiv drept generator. Fie acesta* $\alpha = (0, 9)$. *Calculăm "puterile" lui* α *(de fapt multiplii, grupul fiind aditiv). Pentru* 2α *se calculează întâi (modulo* 19*):*

$$\lambda = (3 \cdot 0^2 + 1)(2 \cdot 9)^{-1} = 1 \cdot 18^{-1} = 18.$$

Acum se pot determina
$x_3 = 18^2 - 0 - 0 = 361 \equiv 1 \ (mod\ 19), \quad y_3 = 18 \cdot (0 - 1) - 9 = -27 \equiv 11 \ (mod\ 19)$,
deci $2\alpha = (1, 11)$.
Multiplul următor este $3\alpha = 2\alpha + \alpha = (1, 11) + (0, 9)$. *Avem:*

$$\lambda = (9 - 11) \cdot (0 - 1)^{-1} = 2, \text{ deci}$$

$x_3 = 2^2 - 1 - 0 = 3, \quad y_3 = 2 \cdot (1 - 3) - 11 = -15 \equiv 4 \ (mod\ 19)$,
de unde rezultă $3\alpha = (3, 4)$.
În mod similar se obţin toate punctele curbei eliptice E*:*

$\alpha = (0, 9)$	$2\alpha = (1, 11)$	$3\alpha = (3, 4)$	$4\alpha = (4, 4)$	$5\alpha = (13, 12)$
$6\alpha = (11, 6)$	$7\alpha = (12, 15)$	$8\alpha = (12, 4)$	$9\alpha = (11, 13)$	$10\alpha = (13, 7)$
$11\alpha = (4, 15)$	$12\alpha = (3, 15)$	$13\alpha = (1, 8)$	$14\alpha = (0, 10)$	$15\alpha = \mathcal{O}$

De remarcat că – de exemplu – $(3, 4)$ *nu este element primitiv, având ordinul* 5.

O curbă eliptică definită pe Z_p ($p > 3$ prim) are aproximativ p puncte. Numărul punctelor din $E(Z_p)$ este numit *ordinul lui* E peste Z_p. O teoremă a lui Hasse ([20]) stabileşte un interval pentru acest număr:

$$p + 1 - 2\sqrt{p} \leq card(E(Z_p)) \leq p + 1 + 2\sqrt{p}$$

Valoarea $t = 2\sqrt{p}$ se numeşte *urma lui* E *peste* Z_q, iar intervalul $[p + 1 - t, p + 1 + t]$ este numit *interval Hasse*.

Calculul efectiv al lui $card(E(Z_p))$ este destul de dificil şi vom trece peste el[2]. Există un algoritm al lui *Schoof* ([20], pag 137-140) de numărare a punctelor unei curbe eliptice, dar complexitatea lui este destul de mare: $\mathcal{O}(log^6 p)$ ($\mathcal{O}(log^9 p)$ în versiunea originală) înmulţiri şi inversiuni, şi $\mathcal{O}(log^3 p)$ spaţiu de memorie. În plus implementarea sa este destul de greoaie şi nu a fost realizată complet până în prezent.

În cazul curbelor eliptice construite peste extensii, se poate da următoarea teoremă:

Teorema 10.1. *Fie* $p = q^m$. *Există o curbă eliptică* E *definită peste* Z_p, *cu* $card(E(Z_p)) = p + 1 - t$ *dacă şi numai dacă este verificată una din condiţiile:*

- $t \not\equiv 0 \ (mod\ q)$ *şi* $t^2 \leq 4p$.

[2]Nu se cunoaşte nici o formulă care să dea valoarea $card(E(Z_p))$; există o conjectură *Birch and Swinnerton-Dyer* în legătură cu acest subiect, conjectură inclusă printre cele şapte probleme ale mileniului (împreună cu "problema "P versus NP").

- *m este impar şi*
  - $t = 0$, *sau*
  - $t^2 = 2p$ *şi* $q = 2$, *sau*
  - $t^2 = 3p$ *şi* $q = 3$.
- *m este par şi*
  - $t^2 = 4p$, *sau*
  - $t^2 = p$ *şi* $q \not\equiv 1 \pmod 3$, *sau*
  - $t = 0$ *şi* $q \not\equiv 1 \pmod 4$.

O informaţie utilă referitoare la structura de grup a lui $E(Z_p)$ este dată de teorema următoare:

Teorema 10.2. *(Teorema lui Ruck) Fie E o curbă eliptică peste* Z_p *cu* $p > 3$ *număr prim. Atunci există două numere întregi* n_1, n_2 *astfel ca* $E(Z_p)$ *să fie izomorfă cu* $Z_{n_1} \times Z_{n_2}$, *iar*

$$n_2 | n_1,\ n_2 | (p-1).$$

Demonstraţia poate fi găsită în [20], pag. 107.

O consecinţă a acestei teoreme este evaluarea $card(E(Z_p)) = n_1 \cdot n_2$. Dacă $n_2 = 1$, atunci $E(Z_p)$ este grup ciclic. Dacă $n_2 > 1$, atunci spunem că $E(Z_p)$ are *rangul* 2. Dacă valoarea lui n_2 este mică ($n_2 \leq 4$), spunem că $E(Z_p)$ este *aproape ciclic*. Cum n_2 divide n_1 şi $p-1$, se aşteaptă ca $E(Z_p)$ să fie ciclic sau aproape ciclic pentru majoritatea curbelor eliptice peste Z_p.

10.2 Sisteme de criptare construite pe curbe eliptice

Pe spaţiul curbelor eliptice se pot realiza diverse tehnici de criptare cu cheie publică; unele din ele sunt doar adaptări ale sistemelor deja prezentate, altele sunt aplicaţii specifice.

Principala atracţie a sistemelor construite pe curbe eliptice constă în dimensiuni mici ale cheilor, ceea ce le face aplicabile pe sisteme portabile (smart-carduri de exemplu).

În general, sistemele de criptare se bazează pe problema logaritumuluin discret şi sunt inspirate de algoritmul *El Gamal*.

Exemplul 10.2. *Să vedem cum se realizează o criptare El Gamal pentru curba eliptică definită în Exemplul 10.1.*

Fie $\alpha = (0, 9)$ *şi să presupunem că exponentul secret este* $a = 7$. *Atunci* $\beta = 7\alpha = (12, 15)$, *iar operaţia de criptare este:*

$$e_K(x, k) = (k \cdot (0, 9), x + k \cdot (12, 15)),\ \textit{unde}\ x \in E,\ 0 \leq k \leq 14.$$

Pentru decriptare se foloseşte operaţia

$$d_K(y_1, y_2) = y_2 - 7y_1$$

Să presupunem că Alice vrea să cripteze mesajul $x = (3, 4)$ *(care este un punct din* E*); dacă ea alege aleator valoarea* $k = 8$*, va calcula*

$y_1 = 8 \cdot (0, 9) = (12, 4)$*, şi*

$y_2 = (3, 4) + 8 \cdot (12, 15) = (3, 4) + (4, 15) = 3\alpha + 8 \cdot 7\alpha = 3\alpha + 11\alpha = 14\alpha = (0, 10)$ *(coeficienţii se calculează modulo* 15*).*

Deci $y = ((12, 4), (0, 10))$*. După recepţie, Bob decriptează mesajul astfel:*

$x = (0, 10) - 7 \cdot (12, 4) = 14\alpha - 7 \cdot 8\alpha = 3\alpha$*.*

10.2.1 Sistemul Menezes - Vanstone

În acest sistem de criptare – de fapt o variantă a lui *El Gamal* – curba eliptică este utilizată pentru "mascare", domeniile de valori al textelor clare şi criptate fiind mult mai largi. Prezentarea algoritmului este:

Fie E o curbă eliptică peste Z_p ($p > 3$ prim) care conţine un subgrup ciclic H în care problema logaritmului discret este dificilă.
Alegem $\mathcal{P} = Z_p^* \times Z_p^*$, $\mathcal{C} = E \times Z_p^* \times Z_p^*$ şi

$$\mathcal{K} = \{(E, \alpha, a, \beta) \mid \alpha \in E,\ a \in Z_p^*,\ \beta = a \cdot \alpha\}.$$

Valorile $\alpha,\ \beta$ sunt publice, iar a este secret.
Pentru $K = (E, \alpha, a, \beta)$, $k \in Z_{card(H)}$ ales aleator (secret) şi $x = (x_1, x_2) \in \mathcal{P}$, definim

$$e_K(x, k) = (y_0,\ y_1,\ y_2),$$

unde $y_0 = k \cdot \alpha, \quad (c_1, c_2) = k \cdot \beta, \quad y_i = c_i \cdot x_i\ (mod\ p), i = 1, 2.$
Pentru un text criptat $y = (y_0, y_1, y_2)$ se defineşte

$$d_K(y) = (y_1 \cdot c_1^{-1}\ (mod\ p),\ y_2 \cdot c_2^{-1}\ (mod\ p)),$$

unde $a \cdot y_0 = (c_1, c_2)$.

Exemplul 10.3. *Revenind la curba* $y^2 = x^3 + x + 5$ *peste* Z_{19} *definită în Exemplul 10.1, criptarea Menezes - Vanstone autorizează* $18 \cdot 18 = 324$ *texte clare, faţă de numai* 15 *în sistemul El Gamal adaptat.*

Să luăm din nou $\alpha = (0, 9)$ *şi exponentul* $a = 7$*. Atunci* $\beta = 7 \cdot \alpha = (12, 15)$*.*

Dacă Alice doreşte să transmită textul clar $x = (x_1, x_2) = (5, 11)$ *(de remarcat că acesta nu este un punct din* E*) şi alege* $k = 4$*, ea va începe prin a calcula*

$$y_0 = k \cdot \alpha = 4 \cdot (2, 7) = (4, 4) şi k \cdot \beta = 4(12, 15) = (1, 8)$$

deci $c_1 = 1,\ c_2 = 8$.

Apoi se calculează (modulo 19*):*

$$y_1 = c_1 \cdot x_1 = 1 \cdot 5 = 5 \text{ şi } y_2 = c_2 \cdot x_2 = 8 \cdot 11 = 12.$$

Alice trimite deci lui Bob mesajul criptat $y = (y_0,\ y_1,\ y_2) = ((4,4), 5, 12)$.

După recepţie, Bob calculează $(c_1,\ c_2) = a \cdot y_0 = 7 \cdot (4,4) = 7 \cdot 4\alpha = 13 \cdot \alpha = (1,8)$*, apoi*

$$x = (y_1 \cdot c_1^{-1}\ (mod\ 19),\ y_2 \cdot c_2^{-1}\ (mod\ 19)) = (5 \cdot 1^{-1},\ 12 \cdot 8^{-1}) = (5,\ 12 \cdot 12) = (5, 11).$$

10.3 Problema logaritmului discret pe curbe eliptice

După cum am văzut anterior, principalele sisteme de criptare pe curbe eliptice folosesc problema logaritmului discret. În cazul curbelor eliptice, ea se enunţă în felul următor:

Problema logaritmului discret pe curbe eliptice (ECDLP):
Fiind dată o curbă eliptică E peste corpul Z_p, un punct $P \in E(Z_p)$ de ordin n şi $Q \in [P] = \{sP \mid 1 \leq s \leq n-1\}$, să se determine k astfel încât $Q = kP$.
Numărul k este numit *logaritmul discret al lui* A *în baza* P : $k = log_P Q$.

Vom prezenta o serie de atacuri generale asupra $ECDLP$, atacuri care nu exploatează eventuale slăbiciuni particulare ale anumitor curbe eliptice. Deoarece ele au fost detaliate pentru sistemele de criptare *El Gamal* sau RSA, vom detalia doar modalitatea lor de scriere în cazul curbelor eliptice.

10.3.1 Atacul Pohlig - Hellman

Cea mai simplă metodă de atac este prin forţă brută: se calculează $R = kP$ pentru $k = 1, 2, 3, \ldots$, verificându-se permanent egalitatea $R = Q$. Atunci când egalitatea este verificată, s-a găsit valoarea $k = log_P Q$. Algoritmul nu solicită multă memorie, dar timpul de rulare este $\mathcal{O}(n)$, unde n este ordinul lui P.

Pohlig şi Hellman au observat că problema logaritmului discret într-un grup G are acelaşi ordin de dificultate ca şi problema logaritmului discret în cel mai mare subgrup prim din G. Ca o consecinţă pentru criptografia pe curbe eliptice, se vor selecta curbe eliptice E cu proprietatea $card(E(Z_p)) = n = h \cdot s$, unde s este un număr prim mare, iar h este un număr foarte mic (de obicei $h = 1, 2$ sau 4). În acest caz, $ECDLP$ este dificilă.

Ideile de bază ale atacului Pohling - Hellman (adaptate criptografiei pe curbe eliptice) sunt:

Fie $n = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$.
1. Se calculează $k_i = k \ (mod\ p_i^{e_i})$ $(1 \le i \le r)$.
2. Se rezolvă sistemul de congruenţe

$$x \equiv k_i \ (mod\ p_i^{e_i}) \qquad (1 \le i \le r).$$

Teorema chineză a resturilor asigură existenţa unei soluţii unice $k = x \in [0, n-1]$.

Să arătăm că determinarea fiecărui k_i se poate reduce la aflarea exponentului e_i într-un subgrup ciclic $[P]$ de ordin p_i; pentru simplificare, vom nota p_i cu p.

Să reprezentăm k_i în baza p; vom avea $k_i = \sum_{j=0}^{e_i-1} z_j p^j$, unde $z_j \in [0, p-1]$.

Pentru determinarea lui z_0:

- Se calculează $P_0 = (n/p)P, \quad Q_0 = (n/p)Q$;
- Deoarece ordinul lui P_0 este p, avem $Q_0 = \frac{n}{p}Q = k\left(\frac{n}{p}P\right) = kP_0 \equiv z_0 P_0 \ (mod\ p)$

Deci $z_0 = log_{P_0} Q_0$ poate fi obţinut rezolvând o instanţă $ECDLP$ în grupul ciclic $[P]$.

La pasul următor se determină $Q_1 = \left(\frac{n}{p^2}\right)(Q - z_0 P)$. Vom avea:

$$Q_1 = \left(\frac{n}{p^2}\right)(Q - z_0 P) = \frac{n}{p^2}(k - z_0)\, P = (k - z_0)\left(\frac{n}{p^2}P\right) = (z_0 + z_1 p - z_0)\left(\frac{n}{p^2}P\right) =$$
$$= z_1\left(\frac{n}{p}P\right) \equiv z_1 P_0 \quad (mod\ p)$$

Valoarea $z_1 = log_{P_0} Q_1$ se poate obţine deci rezolvând o instanţă $ECDLP$ în $[P]$.

În general, dacă numerele $z_0, z_1, \dots, z_{t-1}$ au fost calculate, atunci $z_t = log_{P_0} Q_t$, unde

$$Q_t = \frac{n}{p^{t+1}}\left(Q - z_0 P - z_1 pP - z_2 p^2 P - \dots - z_{t-1} p^{t-1} P\right).$$

Pentru detalii referitoare la corectitudinea algoritmului, se poate relua secţiunea 9.2.2 care tratează algoritmul Pohlig - Hellman în varianta generală.

10.3.2 Atacul $BSGS$ (Baby-Step/Giant-Step)

Ca o consecinţă a atacului Pohlig Hellman, ne putem concentra atenţia asupra rezolvării problemei logaritmului discret în grupuri ciclice de ordin prim. Atacul $BSGS$ este atacul Shanks (prezentat în secţiunea 9.2.1) adaptat pentru curbe eliptice.

Fie $G = [P]$ un subgrup ciclic de ordin p (p prim) al unui grup $E(Z_q)$ al unei curbe eliptice. Fiind dat $Q \in G$, problema cere aflarea unei valori k $(1 \le k < p)$ astfel încât $Q = kP$.

Considerăm reprezentarea

$$k = k_0 + k_1\lfloor\sqrt{p}\rfloor$$

unde $k_0, k_1 \in [0, \lfloor\sqrt{p}\rfloor)$.

1. Se calculează lista $A = \{(P_i, i) \mid P_i = iP, \quad 0 \leq i < \lfloor\sqrt{p}\rfloor\}$ (faza "Baby - Step").
2. Fie $R = \lfloor\sqrt{p}\rfloor P$. Se calculează lista $B = \{(Q_j, j) \mid Q_j = Q - jR, \quad 0 \leq j < \lfloor\sqrt{p}\rfloor\}$ (faza "Giant - Step").

   Cele două liste sunt ordonate crescător după prima componentă.
3. Se caută $(P_i, i) \in A$, $(Q_j, j) \in B$ astfel ca $P_i = Q_j$.
   Dacă aşa ceva există, atunci $k_0 = i$, $k_1 = j$.

Justificare: Avem $iP = Q - j\lfloor\sqrt{p}\rfloor P$, deci $(i + j\lfloor\sqrt{p}\rfloor)P = Q$.

După cum se ştie, complexitatea spaţiu şi complexitatea timp a unui astfel de atac sunt ambele egale cu $\mathcal{O}(\lfloor\sqrt{p}\rfloor)$. Shoup ([49]) arată că atacul $BSGS$ este cea mai rapidă metodă pentru rezolvarea problemei logaritmului discret într-un grup "cutie neagră"[3].

10.3.3 Atacul Pollard Rho

Ideea de bază în algoritmul Pollard Rho constă în găsirea a două perechi distincte (c_1, d_1), (c_2, d_2) de numere întregi din Z_p astfel încât

$$c_1P + d_1Q = c_2P + d_2Q.$$

De aici va rezulta $(c_1 - c_2)P = (d_2 - d_1)Q = (d_2 - d_1)kP$, deci

$$(c_1 - c_2) \equiv (d_2 - d_1)k \pmod{p},$$

şi valoarea $k = log_PQ$ se obţine imediat prin

$$k = (c_1 - c_2)(d_2 - d_1)^{-1} \pmod{p}$$

O metodă ingenioasă de aflare a unor astfel de perechi constă în selectarea aleatoare a două valori $c, d \in Z_p$ şi memorarea într-o tabelă a tripletului $(c, d, cP + dQ)$. Procedeul se repetă (tabela se completează eventual sortată după a treia componentă), până se obţine a doua oară un punct $cP + dQ$.

[3]Un grup "cutie neagră" este un grup în care nu se foloseşte nici o structură prestabilită pentru reprezentarea elementelor sale.

Neajunsul acestui atac constă în necesitatea de stocare a $\sqrt{\pi p/2}$ triplete.

Algoritmul Pollard Rho găseşte perechile $(c_1, d_1), (c_2, d_2)$ cam în acelaşi timp ca şi metoda de mai sus, dar folosind o cantitate neglijabilă de memorie. Ideea – similară celei din secţiunea 9.2.3 – este de a defini o funcţie recursivă $f : [P] \longrightarrow [P]$ astfel încât, fiind dat $X \in [P]$ şi $c, d \in Z_p$ cu $X = cP + dQ$, sunt uşor de calculat $X' = f(X)$ şi $c', d' \in Z_p$ cu $X' = c'P + d'Q$.

În plus, f ar trebui să aibă caracteristicile unei funcţii aleatoare.

Algoritmul Pollard Rho este:

Intrare: $P \in E(Z_q)$, $ord(P) = p$ număr prim, şi $Q \in [P]$.
Ieşire: $k = log_P Q$.
1. Selectează numărul L al ramificaţiilor (în 9.2.3 s-a definit apriori $L = 3$).
2. Selectează o funcţie de partiţie $H : [P] \longrightarrow \{1, 2, \ldots, L\}$ cu proprietatea $card(H^{-1}(i)) \simeq p/L$, $(1 \leq i \leq L)$.
3. **for** $j \longleftarrow 1$ **to** L **do**
   3.1. Selectează (aleator) $a_j, b_j \in Z_p$.
   3.2. Calculează $R_j = a_j P + b_j Q$.
4. Selectează (aleator) $c', d' \in Z_p$ şi calculează $X' = c'P + d'Q$.
5. $X" \longleftarrow X'$, $c" \longleftarrow c'$, $d" \longleftarrow d'$.
6. **repeat**
   6.1. Calculează $j = H(X')$.
   $X' \longleftarrow X' + R_j, \quad c' \longleftarrow c' + a_j \ (mod\ p), \quad d' \longleftarrow d' + b_j \ (mod\ p)$.
   6.2. **for** $i \longleftarrow 1$ **to** 2 **do**
   6.2.1. Calculează $j = H(X")$.
   $X" \longleftarrow X" + R_j, \quad c" \longleftarrow c" + a_j \ (mod\ p), \quad d" \longleftarrow d" + b_j \ (mod\ p)$.
   until $X' = X"$.
7. **if** $d' = d"$ **then return**("eşec")
   else return $k = (c' - c")(d" - d')^{-1} \ (mod\ p)$.
8. **Stop**

După cum se observă, algoritmul Pollard Rho este un algoritm probabilist de tip Las Vegas. Probabilitatea de eşec este neglijabilă.

Exemplul 10.4. *Să considerăm $L = 32$ şi fie $\{S_1, S_2, \ldots, S_{32}\}$ o partiţie a lui $[P]$ definită astfel: dacă $X \in [P]$ şi ultimii ultimii 5 biţi semnificativi ai primei coordonate a lui X reprezintă numărul j, atunci $H(X) = j + 1$. Mulţimile $S_j = \{X \mid H(X) = j\}$ au acelaşi număr de elemente pentru orice $j = 1, 2, \ldots, 32$.*

Să detaliem puţin algoritmul Pollard Rho:
Fie $a_j, b_j \in Z_p$. Se defineşte funcţia $f : [P] \longrightarrow [P]$ prin

$$f(X) = X + a_j P + b_j Q \quad \text{unde} \quad j = H(X).$$

Se observă că dacă $X = cP + dQ$, atunci $f(X) = X' = c'P + d'Q$ unde $c' = c + a_j \ (mod\ p)$ şi $d' = d + b_j \ (mod\ p)$.

Acum, pentru un punct arbitrar $X_0 \in [P]$ se poate determina o secvenţă de puncte $\{X_i\}_{i\geq 0}$ definită $X_i = f(X_{i-1})$ pentru $i \geq 1$.

Cum toate aceste puncte sunt din grupul finit $[P]$, la un moment dat secvenţa va începe să se repete (şi să cicleze). Deci există un t minim pentru care $X_t = X_{t+s}$ cu $s \geq 1$. Valoarea t se numeşte "*lungimea cozii*", iar s – "*lungimea ciclului*".

Dacă f este o funcţie cu proprietăţi aleatoare, atunci $t \simeq \sqrt{\pi p/8}$, $s \simeq \sqrt{\pi p/8}$, deci secvenţa va începe să se repete după aproximativ $\sqrt{\pi p/2}$ termeni.

Algoritmul lui Floyd de aflare a două puncte X_i, X_j cu $X_i = X_j$ şi $i \neq j$, explorează perechile de puncte de forma (X_i, X_{2i}) până găseşte un indice i cu $X_i = X_{2i}$. După calcularea unei perechi, perechea anterioară de puncte poate fi eliminată; astfel memoria utilizată este de mărime neglijabilă. Numărul n al perechilor calculate până se obţine egalitatea $X_i = X_{2i}$ verifică relaţia $t \leq n \leq t + s$. Dacă f este o funcţie aleatoare, atunci $n \simeq 1,0308\sqrt{p}$, deci numărul de operaţii pe grupul curbelor eliptice este $3\sqrt{p}$.

10.4 Factorizări bazate pe curbe eliptice

În cadrul sistemului de criptare RSA la secţiunea 8.4.4. a fost prezentată metoda $p-1$ de factorizare a unui număr. Ideea sa era de a efectua operaţii într-un grup Z_p^* sensibil mai mic decât grupul multiplicativ Z_n^* (unde p este un divizor al lui n) în care sunt definite toate calculele. Această concepţie – de a restrânge de facto domeniul de calcul – poate fi extinsă şi la alte grupuri, în particular la grupul definit pe mulţimea punctelor unei curbe eliptice. Metoda folosită este numită ECM (Elliptic Curve Method) şi este descrisă mai jos.

Să generăm aleator două numere $a, b \in Z_n$, şi să construim curba $E_{a,b}$ de ecuaţie

$$y^2 \equiv x^3 + ax + b \ (mod\ n) \tag{8}$$

Vom considera pe această curbă diverse calcule modulo p (deşi p nu se cunoaşte), calcule "ascunse" de calculele modulo n. Ordinul grupului $E_{a,b}(Z_p)$ este un număr aleator în intervalul $[p + 1 - 2\sqrt{p}, p + 1 + 2\sqrt{p}]$. Dacă acest ordin are divizorii primi (la puterile cu care apar) mai mici decât marginea B stabilită de metoda $p-1$, putem aplica această metodă (adaptată la grupul definit pe $E(Z_n)$), cu o complexitate de $\mathcal{O}(B)$ operaţii aritmetice. Succesul ei corespunde deci probabilităţii ca ordinul grupului $E_{a,b}(Z_p)$ să aibă toţi divizorii primi mai mici decât B. Această probabilitate este estimată în [31] la u^{-u} unde $u = \dfrac{log\ p}{log\ B}$.

Exemplul 10.5. *Să încercăm factorizarea numărului $n = 44023$ (pentru care metoda $p-1$ definită în 8.4.4. eşuează).*

Prima problemă care apare este alegerea unui punct (iniţial) X pe curba (8). *Această alegere nu este simplă, deoarece trebuie să rezolvăm o ecuaţie algebrică modulo un număr n a cărui factorizare nu se cunoaşte. Pentru a evita această dificultate, în loc de a alege a, b şi apoi X, vom genera întâi a, X şi ulterior b.*

Să alegem $a = 13$ şi $X = (x, y) = (23482,\ 9274)$. Vom avea imediat

$$b = y^2 - x^3 - ax \equiv 21375 \pmod{44203}$$

Conform metodei $p-1$, vom calcula $X_i = i!X = (x_i, y_i)$ pentru $i = 1, 2, \ldots$ până se ajunge la un punct $X_i \neq \mathcal{O}$ (în $E_{a,b}(Z_n)$), care este punctul de la infinit în $E_{a,b}(Z_p)$. Aceste lucru se poate întâmpla la apariţia unei operaţii imposibile – de obicei împărţirea la un element neinversabil. Elementele neinversabile din Z_n^* conduc, prin calcularea unui cel mai mare divizor comun, la un factor al lui n (deci la factorizare).

Determinarea lui X_1 este uşoară: $X_1 = X = (23482,\ 9274)$. Urmează:

$X_2 = 2X_1 = (18935,\ 21838)$,

$X_3 = 3X_2 = 2X_2 + X_2 = (15187,\ 29168)$,

$X_4 = 4X_3 = 2(2X_3) = (10532,\ 5412)$

şi ajungem la $X_5 = 5X_4 = 2(2X_4) + X_4$.

Aici calculăm întâi $2X_4 = (30373,\ 40140)$, apoi $2(2X_4) = (27556,\ 42335)$.

În momentul când vrem să adunăm acest punct cu X_4, ajungem la calculul valorii

$$\lambda = \frac{42335 - 5412}{27556 - 10532} \pmod{44023}$$

care nu se poate efectua, deoarece $27556 - 10532 = 17024$ nu este inversabil modulo n. Atunci când încercăm să calculăm inversul folosind algoritmul lui Euclid extins, ajungem la $cmmdc(17024, 44023) = 133$, care este un factor al lui $n = 44023$.

10.5 Exerciţii

10.1. *Să se verifice propietăţile de grup ale operaţiei aditive definite pe $E(L)$.*

10.2. *Fie E curba eliptică $y^2 = x^3 + x + 28$ peste Z_{71}.*

1. *Determinaţi numărul de puncte din $E(Z_{71})$;*
2. *Arătaţi că grupul $E(Z_{71})$ nu este ciclic;*
3. *Care este ordinul maxim al unui element din $E(Z_{71})$? Găsiţi un astfel de element.*

10.3. *Fie E curba eliptică $y^2 = x^3 + x + 13$ definită pe Z_{31}. Se poate arăta că $E(Z_{31})$ are 34 puncte şi că $(9, 10)$ este de ordinul 34 în E. Sistemul de criptare Mezenes - Vanstome definit pe E admite ca spaţiu al textelor clare $Z_{34}^* \times Z_{34}^*$. Fie $a = 25$ exponentul secret al lui Bob.*

1. *Calculaţi* $\beta = a \cdot \alpha$*;*

2. *Decriptaţi textul următor:*

$$((4,9),28,7)((19,28),9,13)((5,22),20,17)((25,16),12,27)$$

3. *Dacă presupunem că fiecare text clar reprezintă două caractere alfabetice, convertiţi acest text clar în engleză (s-a folosit corespondenţa* $A-1,\ \ldots,\ Z-26$*).*

10.4. *Fie* E *curba eliptică* $y^2 = x^3 + x + 6$ *peste* Z_{11}*.*

(*a*) *Să se calculeze punctele lui* $E(Z_{11})$*.*

(*b*) *Se aleg parametrii* $\alpha = (2,7)$ *şi* $a = 7$*. Folosind sistemul de criptare El Gamal, să se cripteze mesajul* $x = (10,9)$ *cu valoarea aleatoare* $k = 3$*.*

(*c*) *Folosind sistemul de criptare Menezes - Vanstone şi aceiaşi parametri, să se cripteze mesajul* $x = (9,1)$*.*

10.5. *Fie* $p > 3$ *un număr prim impar şi* $a, b \in Z_p$*. Dacă ecuaţia* $x^3 + ax + b \equiv 0 \ (mod\ p)$ *are trei rădăcini distincte în* Z_p*, arătaţi că grupul curbei eliptice corespunzătoare* $(E, +)$ *nu este ciclic.*

10.6. *Fie* E *o curbă eliptică definită peste* Z_p *unde* $p > 3$ *este un număr prim. Să presupunem că* $n = card(E)$ *este prim şi fie* $P \in E,\ P \neq \mathcal{O}$*.*

(*a*) *Arătaţi că* $log_P(-P) = n - 1$*.*

(*b*) *Daţi un algoritm de calcul pentru* n *de complexitate* $\mathcal{O}(p^{1/4})$ *folosind teorema lui Hasse şi algoritmul BSGS.*

10.7. *Fie curba eliptică* $y^2 = x^3 + 9x + 17$*. Un generator al lui* $E(Z_{23})$ *este* $P = (16,5)$*. Să se calculeze logaritmul punctului* $Q = (4,5)$*.*

10.8. *O reprezentare binară* $(a_{n-1}, a_{n-2}, \ldots, a_0)$ *a numărului întreg* a *este în "forma neadiacentă" (forma* NAF*) dacă nu există două valori consecutive nenule.*

(*a*) *Daţi un algoritm de reprezentare a numerelor întregi în forma* NAF*. Aplicaţi acest algoritm pentru numerele* $87,\ 112,\ 2047$*.*

(*b*) *Folosind reprezentarea* NAF *a lui* 87*, calculaţi* $87P$*, unde* $P = (2,6)$ *este un punct pe curba eliptică* $y^2 = x^3 + x + 26$ *definită peste* Z_{27}*.*

Bibliografie

[1] Anderson R. ş.a. - *Serpent: A proposal for the Advanced Encryption Standard*, http://www.ftp.cl.cam.ac.uk/ftp/users/rja14/serpent.pdf

[2] Atanasiu A. - *Teoria codurilor corectoare de erori*, Editura Univ. Bucureşti, 2001;

[3] Atanasiu, A. - *Arhitectura calculatorului*, Editura Infodata, Cluj, 2006;

[4] Blum L., Blum M., Shub M. - *Comparision of two pseudo-random number generators*, Advanced in Cryptology, CRYPTO 82

[5] D. Bayer, S. Haber, W. Stornetta; Improving the efficiency and reliability of digital time-stamping. Sequences II, Methods in Communication, Security and Computer Science, Springer Verlag (1993), 329-334.

[6] Biham E., Shamir A. - *Differential Cryptanalysis of DES - like Cryptosystems*, Journal of Cryptology, vol. 4, 1 (1991), pp. 3-72.

[7] Biham E., Shamir A. - *Differential Cryptanalysis of the Data Encryption Standard*, Springer-Verlag, 1993.

[8] Biham E., Shamir A. - *Differential Cryptanalysis of the Full 16-Round DES*, Proceedings of Crypto92, LNCS 740, Springer-Verlag.

[9] Biham E. - *On Matsuis Linear Cryptanalysis*, Advances in Cryptology - EUROCRYPT 94 (LNCS 950), Springer-Verlag, pp. 341-355, 1995.

[10] Biryukov A., Shamir A., Wagner D. - *Real Time Cryptanalysis of A5/1 on a PC*, Fast Software Encryption - FSE 2000, pp 118.

[11] Bruen A., Forcinito M - *Cryptography, Information Theory, and Error - Correction*, Wiley Interscience 2005.

[12] Brigitte Collard - *Secret Language in Graeco-Roman antiquity* (teză de doctorat) $http://bcs.fltr.ucl.ac.be/FE/07/CRYPT/Intro.html$

[13] Cook S., *http : //www.claymath.org/millennium/P_vs_NP/Official_Problem_Description.pdf*

[14] Coppersmith D. ş.a. - *MARS - a candidate cypher for AES*, http://www.research.ibm.com/security/mars.pdf

[15] Daemen J., Rijmen V. - *The Rijndael Block Cipher Proposal*, http://csrc.nist.gov/CryptoToolkit/aes/

[16] Damgard I.B. - *A design principle for hash functions*, Lecture Notes in Computer Science, 435 (1990), 516-427.

[17] Diffie D.W., Hellman M.E. - *New Directions in Cryptography*, IEEE Transactions on Information Theory, IT-22, 6 (1976), pp. 644-654

[18] Diffie D.W., Hellman M.E. - *Multiuser cryptographic techniques*, AFIPS Conference Proceedings, $45(1976), 109 - 112$

[19] L´ Ecuyer P. - *Random Numbers for Simulation*, Comm ACM 33, 10(1990), 742-749, 774.

[20] Enge A. - *Elliptic Curves and their applications to Cryptography*, Kluwer Academic Publ, 1999

[21] El Gamal T. - *A public key cryptosystem and a signature scheme based on discrete algorithms*, IEEE Transactions on Information Theory, 31 (1985), 469-472

[22] Fog A. - *http://www.agner.org/random/theory*;

[23] Gibson J. - *Discrete logarithm hash function that is collision free and one way.* IEEE Proceedings-E, 138 (1991), 407-410.

[24] Heyes H. M. - *A Tutorial on Linear and Differential Cryptanalysis.*

[25] van Heyst E., Petersen T.P. - *How to make efficient fail-stop signatures*, Lecture Notes in Computer Science, $658(1993), 366 - 377$

[26] Junod P. - *On the complexity of Matsuiş attack*, in SAC 01: Revised Papers from the 8th Annual International Workshop on Selected Areas in Cryptography, pp 199211, London, UK, 2001. Springer-Verlag.

[27] Kahn D. - *The Codebreakers*, MacMillan Publishing Co, New York, 1967

[28] Kelly T. - *The myth of the skytale*, Cryptologia, Iulie 1998, pp. 244 - 260.

[29] Konheim A. - *Computer Security and Cryptography*, Wiley Interscience, 2007.

[30] Knuth D. - *The art of computer Programming*, vol 2 (Seminumerical Algorithms)

[31] Lenstra, H.W. - *Factoring Integers with Eiipltic Curves*, Annals of Mathematics, vol. 126, pp. 649-673, 1987.

[32] Matsui M, Yamagishi A. - *A new method for known plaintext attack of FEAL cipher.* Advances in Cryptology - EUROCRYPT 1992.

[33] Matsui M. - *Linear Cryptanalysis Method for DES Cipher*, Advances in Cryptology - EUROCRYPT 93, LNCS 765, Springer-Verlag, pp. 386-397, 1994.

[34] Matsui M. - *The first experimental cryptanalysis of the Data Encryption Standard*, in Y.G. Desmedt, editor, Advances in Cryptology - Crypto 4, LNCS 839, SpringerVerlag (1994), 1- 11.

[35] Matsui M. - *New Structure of Block Ciphers with Provable Security against Differential and Linear Cryptalaysis*, Fast Software Encryption, LNCS 1039, Springer-Verlag, 1996, pp. 205-218.

[36] Merkle R. C., Hellman M. - *Hiding Information and Signatures in Trapdoor Knapsacks*, IEEE Trans. IT 24(5), Sept 1978, pp. 525530.

[37] Merkle R.C. - *A fast software one-way functions and DES*, Lecture Notes in Computer Science, 435 (1990), 428-446

[38] Menezes A., Oorschot P., Vanstome S. - *Handbook of Applied Cryptography*, CRC Press 1996.

[39] Preneel B., Govaerts R., Vandewalle J. - *Hash functions based on block ciphers: a syntetic approach*; Lecture Notes in Computer Science, 773 (1994), 368-378

[40] Rivest R. ş.a - *The RC6^{TM} Block Cipher*,
ftp://ftp.rsasecurity.com/pub/rsalabs/rc6/rc6v11.pdf

[41] Rivest R.L. - *The* **MD4** *message digest algorithm*; Lecture Notes in Computer Science, 537, (1991), 303-311

[42] Rivest R., Shamir A., Adleman A. - *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*, Communications of the ACM, Vol. 21 (2), 1978, pages 120–126.

[43] Rosing, M - *Implementing Elliptic Curve Cryptography*, Manning, 1998

[44] D. Salmon - *Data Privacy and Security*, Springer Professional Computing, 2003

[45] Salomaa A. - *Criptografie cu chei publice*, Ed. Militară, Bucureşti 1994

[46] Schneier B. - *Applied Cryptography*, John Wiley and Sons, 1995

[47] Schneier B ş.a. - *Twofish*, http://www.counterpane.com/twofish.html

[48] Shamir, A. - *A polynomial time Algorithm for breaking the basic Merkle - Hellman cryptosystem*,

http://dsns.csie.nctu.edu.tw/research/crypto/HTML/PDF/C82/279.PDF

[49] Shoup, V. - *Lower bounds for discrete logarithm and related problems*, Advanced in Cryptology, EUROCRYPT 97, Springer - Verlag LNCS 1233, pp. 313-328, 1997.

[50] Selmer E.S. - *Linear Recurrence over Finite Field*, Univ. of Bergen, Norway, 1966;

[51] Sibley E.H. - *Random Number Generators: Good Ones are Hard to Find*, Comm ACM 31, 10(1988), 1192-1201.

[52] Smid M.E., Branstad, D.K. - *Response to comments on the NIST proposed digital signature standard*, Lecture Notes in Computer Science, $740(1993), 76 - 88$

[53] Stinton D., *Cryptography, Theory and Practice*, Chapman& Hall/CRC, 2002

[54] Wiener M.J. - *Cryptanalysis of short RSA secret exponents*, IEEE Trans on Information Theory, 36 (1990), 553-558

[55] Williams H.C. - *Some public-key criptofunctions as intractable as factorisation*, Cryptologia, 9 (1985), 224-237.

[56] Zeng K.G., Yang C.H., Wei D.Y., Rao T.R.N.- *Pseudorandom Bit Generators in Stream Cipher Cryptography*, IEEE Computer, 24 (1991), 8.17.

[57] *Secure hash Standard*; National Bureau of Standards, FIPS Publications 180, 1993

[58] $http://en.wikipedia.org/wiki/Enigma\_machine$

[59] $http://en.wikipedia.org/wiki/M-209$

[60] *http://en.wikipedia.org/wiki/Caesar_ cipher# History_ and_ usage*

[61] *http://psychcentral.com/psypsych/Polybius_ square*

[62] *http://www.answers.com/topic/vigen-re-cipher*

[63] *http://en.wikipedia.org/wiki/Rosetta_ stone*

[64] *Serpent homepage*, http://www.cl.cam.ac.uk/ rja14/serpent.html

[65] *P versus NP homepage*, http://www.win.tue.nl/ gwoegi/P-versus-NP.htm

[66] http://www.win.tue.nl/ gwoegi/P-versus-NP.htm

[67] http://en.wikipedia.org/wiki/Complexity_ classes_ P_ and_ NP