SEMINAR IZ KRIPTOGRAFIJE

Drugi javni kriptosistemi (nadaljevanje)

Aleksandar Jurišić (IMFM)

4. maj, 1998

Na zadnjem seminarju:

- Bojan Barlič nadaljuje s 5. poglavjem:
  - Markle-Hellmanov sistem (nahrbtnik)
  - McEliece sistem (error-correcting codes)
- Tomaž Klobučar: rešitve nalog

Današnji načrt

- Drugi javni kriptosistemi (5. pogl.)
  - ElGamalov kriptosistem in diskretni logaritem
  - (že predelali) končni obsegi
  - (že predelali) eliptični kriptosistemi
- Massey-Omura shema
- nekaj novih nalog
- rešitve nalog 4. in 5. poglavja

JAVNA KRIPTOGRAFIJA

L. 1976 sta Whit **Diffie** in Martin **Hellman** predstavila koncept kriptografije z javnimi ključi.

Le-ta za razliko od simetrčnega sistema uporablja dva različna ključa, **privatnega** in pa **javnega**.
V prejšnjem poglavju smo spoznali RSA (1978).

Taher ElGamal (1985): enkripcije z javnimi ključi in sheme digitalnih podpisov.

Varianta: algoritem za digitalni podpis (**Digital Signature Algorithm** – **DSA**), ki ga je prispevala vlada ZDA.

V razvoju javne kriptografije je bilo razbitih veliko predlaganih sistemov.

Le tri vrste so se obdržale in jih lahko danes smatramo za varne in učinkovite.

Glede na matematični problem na katerem temeljijo, so razdeljene v tri skupine:

- **Sistemi faktorizacije celih števil** (Integer Factorization Systems) z RSA (Rivest-Adleman-Shamir) kot najbolj znanim predstavnikom.
- **Sistemi diskretnega algoritma** (Discrete Logarithem Systems), kot na primer DSA.
- **Kripto sistemi z eliptičnimi krivuljami** (Elliptic Curve Cryptosystems)

Problem diskretnega logaritma v grupi G:

za dana $\alpha, \beta \in G$*, kjer je red elementa* α *enak* n*, najdi* $x \in \{0, \ldots, n-1\}$*, tako da je* $\alpha^x = \beta$*.*

Število x se imenuje **diskretni logaritem** osnove α elementa β.

Medtem, ko je diskretni logaritem (verjetno) težko izračunati (v splošnem), lahko potenco izračunamo hitro (primer enosmerne funkcije).

Osnovna razloga za uporabo različnih grup:

- operacije v nekaterih grupah so izvedene enostavneje v programih (software) in programski opremi (hardware) kot v drugih grupah,
- problem diskretnega logaritma je v določeni grupi lahko zahtevnejši kot v drugi.

ElGamal-ovi protokoli

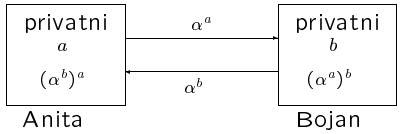
Delimo jih v tri razrede:

1. protokoli za izmenjavo ključev,
2. sistemi z javnimi ključi,
3. digitalni podpisi.

Te protokole lahko uporabimo s poljubno končno grupo G. Naj bo $\alpha \in G$ in naravno število n red tega elementa (t.j., $\alpha^n = 1$ in $\alpha^k \neq 1$ za vsak $k < n$).

1. IZMENJAVA KLJUČEV

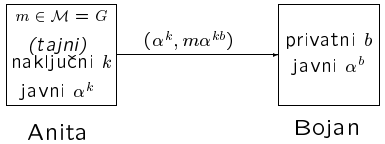
(Diffie-Hellman)



Anita in Bojan si delita skupni element grupe: $(\alpha^a)^b = (\alpha^b)^a = \alpha^{ab}$.

2. SISTEM JAVNIH KLJUČEV

(dva ključa, asimetrični sistem)



Sporočilo m lahko prebere le Bojan, ni pa nikjer rečeno, da mu ga je res poslala Anita (saj ni uporabila svojega privatnega ključa).

V javni kriptografiji smatramo, da nam javni del (npr. α^k, α^b) v ničemer ne pomaga pri iskanju tajnega/privatnega dela (npr. k, b).

(Digitalni podpis bo obravnavan v 6. poglavju.)

Zgled:
za G si izberemo grupo $GF(23)^*$.

Elementi obsega $GF(23)$ so: $0, 1, \ldots, 22$.

Definirajmo:
$a + b = r_1$, kjer je r_1 vsota $a + b$ mod 23.
$ab = r_2$, kjer je r_2 produkt ab mod 23.

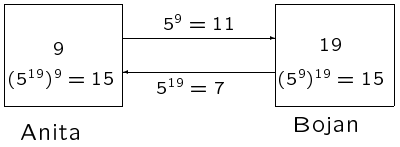
Primer: $12 + 20 = 32 = 9$, $8 \cdot 9 = 72 = 3$.

Multiplikativna grupa $GF(23)^*$

Elementi $GF(23)^*$ so elementi $GF(23)\backslash\{0\}$, in jih lahko generiramo z enim elementom:

$5^0 = 1$	$5^8 = 16$	$5^{16} = 3$
$5^1 = 5$	$5^9 = 11$	$5^{17} = 15$
$5^2 = 2$	$5^{10} = 9$	$5^{18} = 6$
$5^3 = 10$	$5^{11} = 22$	$5^{19} = 7$
$5^4 = 4$	$5^{12} = 18$	$5^{20} = 12$
$5^5 = 20$	$5^{13} = 21$	$5^{21} = 14$
$5^6 = 8$	$5^{14} = 13$	$5^{22} = 1$
$5^7 = 17$	$5^{15} = 19$	

Diffie–Hellmanov protokol v $GF(23)^*$



Anita in Bojan si sedaj delita skupen element $5^{9 \cdot 19} = 15$.

Log tabela

log	elt	log	elt	log	elt
0	1	8	16	16	3
1	5	9	11	17	15
2	2	10	9	18	6
3	10	11	22	19	7
4	4	12	18	20	12
5	20	13	21	21	14
6	8	14	13		
7	17	15	19		

Grupo G in generator α si izberemo tako, da je red elementa α velik (s tem pa je velika tudi log tabela).

Antilog tabela

elt	log	elt	log	elt	log
1	0	9	10	17	7
2	2	10	3	18	12
3	16	11	9	19	15
4	4	12	20	20	5
5	1	13	14	21	13
6	18	14	21	22	11
7	19	15	17		
8	6	16	8		

Algoritmi za računanje diskretnega logaritma

- Shankov algoritem
  (veliki korak – mali korak),
- Pollardov ρ algoritem,
- Pohlig-Hellmanov algoritem,
- metoda "index calculus".

Zadnjič smo si na hitro ogledali prvi in zadnji algoritem.

Metoda veliki korak – mali korak:
$GF(23)^*$ z gen. 5: sestavi tabelo elementov $5^0, 5^5, 5^{10}, 5^{15}, 5^{20}$ in njihovih logaritmov.

element	1	20	9	19	12
logaritem	0	5	10	15	20

Izračunaj log(18): računaj $5 \times 18, 5^2 \times 18, \cdots$ vse dokler ne dobiš element iz tabele.
$5 \times 18 = 21$, $5^2 \times 18 = 13$, $5^3 \times 18 = 19$.
Iz tabele dobimo $\log(5^3 \times 18) = \log 19 = 15$.
Sledi $3 + \log 18 = 15$ oziroma $\log 18 = 12$.

$GF(89)^*$ z generatorjem 3: sestavi tabelo elementov $3^0, 3^{10}, 3^{20}, \cdots, 3^{80}$ in njihovih algoritmov.

elt	1	42	73	40	78	72	87	5	32
log	0	10	20	30	40	50	60	70	80

Izračunaj log(36): računaj $3 \times 36, 3^2 \times 36, \cdots$ vse dokler ne dobiš element iz tabele.
$3 \times 36 = 19$, $3^3 \times 36 = 82$, $3^5 \times 36 = 26$, $3^2 \times 36 = 57$, $3^4 \times 36 = 68$, $3^6 \times 36 = 78$.
Iz tabele preberemo $\log(3^6 \times 36) = \log 78$.
Sledi $6 + \log 36 = 40$ oziroma $\log 36 = 34$.

Povzetek:
metoda veliki korak – mali korak:

Daljša je tabela, ki jo sestavimo, dlje časa jo je bilo treba računati (enkratni strošek), po drugi strani pa hitreje naletimo na element v tabeli.

Običajno sestavimo tabelo velikosti $m = \lfloor \sqrt{|G|} \rfloor$ in za iskanje potrebujemo $O(m)$ časa.

Pollardov ρ algoritem
(in Floydov algoritem za iskanje ciklov):

ima isto časovno zahtevnost kot metoda veliki korak – mali korak, porabi pa le malo spomina.

Diskretni logaritem v $\mathbb{Z}_p$:
p praštevilo, $\alpha \in \mathbb{Z}_p$ je primitiven element (i.e., za $n = p - 1$ je $\alpha^n = 1$ in $\alpha^k \neq 1$ for $k < n$), $\beta \in \mathbb{Z}_p$.

Najdi natanko določeno število a,
$0 \geq a \geq p - 2$, za katerega velja

$$\alpha^a \equiv \beta \pmod{p}.$$

Kot običajno pišemo $a = \log_\alpha \beta$, le da gre tu za diskretni logaritem, ki ga ne znamo izračunati s približki kot v realnih številih.

Pohlig-Hellmanov algoritem:

$$p - 1 = \Pi_{i=1}^{k} p_i^{c_i}$$

za različna praštevila p_i. Vrednost $a = \log_\alpha \beta$ je natanko določena po modulu $p - 1$.

Najprej izračunamo a mod $p_i^{c_i}$ za vsak $i = 1, \ldots, k$ in nato izračunamo a mod $(p-1)$ po metodi kitajskih ostankov.

Predpostavimo, da q praštevilo in c največje naravno število za katero velja

$$p - 1 \equiv 0 \pmod{q^c}.$$

Kako izračunamo

$$x = a \bmod q^c, \quad \text{kjer je } 0 \le x \le q^c - 1?$$

Zapišimo x v številskem zapisu z osnovo q:

$$x = \sum_{i=0}^{c-1} a_i q^i, \quad \text{kjer je } 0 \le a_i \le q - 1.$$

Od tod dobimo

$$a = a_0 + a_1 q + \ldots + a_{c-1} q^{c-1} + s q^c,$$

kjer je s neko naravno število in $a = a_0 + Kq$.
a_0 izračunamo iz naslednje identitete

$$\beta^{(p-1)/q} \equiv \alpha^{a_0 (p-1)/q} \bmod p.$$

Dokažimo slednjo kongruenco:

$$\begin{aligned} \beta^{(p-1)/q} &\equiv (\alpha^a)^{(p-1)/q} \bmod p \\ &\equiv (\alpha^{a_0 + Kq})^{(p-1)/q} \bmod p \\ &\equiv \alpha^{a_0 (p-1)/q}\ \alpha^{(p-1)K} \bmod p \\ &\equiv \alpha^{a_0 (p-1)/q} \bmod p. \end{aligned}$$

Najprej torej izračunamo

$$\beta^{(p-1)/q} \bmod p.$$

Če je $\beta^{(p-1)/q} \equiv 1 \bmod p$, je $a_0 = 0$,
sicer pa zaporedoma računamo

$$\gamma = \alpha^{(p-1)/q} \bmod p, \quad \gamma^2 \bmod p, \quad \ldots,$$

vse dokler ne dobimo

$$\gamma^i \bmod p = \beta^{(p-1)/q} \bmod p$$

in je $a_0 = i$.

Sedaj moramo določiti $a_1, \ldots, a_{c-1}$
(če je $c > 1$). Naj bo

$$\beta_j = \beta \alpha^{a_0 + a_1 q + \ldots + a_{j-1} q^{j-1}} \bmod p,$$

za $0 \le j \le c - 1$. Tokrat velja splošnejša identiteta

$$(\beta_j)^{(p-1)/q^{j+1}} \equiv \alpha^{a_j (p-1)/q} \bmod p,$$

ki jo dokažemo na isti način kot prejšnjo.

Za dani β_j ni težko izračunati a_j, omenimo pa še rekurzijo

$$\beta_{j+1} = \beta_j \alpha^{-a_j q^j} \bmod p.$$

Za dano faktorizacijo števila n, je časovna zahtevnost Pohlig-Hellmanovega algoritma $O(\sum_{i=0}^{k}\ c_i(\log n + \sqrt{p_i})$ grupnih multiplikacij.

Primer: naj bo $p = 251$, potem je

$$n = p - 1 = 250 = 2 \cdot 5^3.$$

Naj bo $\alpha = 71$ in $\beta = 210$,
torej želimo izračunati $a = \log_{71} 210$.

Modul 2: $\gamma_0 = 1$,

$$\gamma_1 \equiv \alpha^{250/2} \equiv 250 \bmod p$$

in

$$\beta^{250/2} \equiv 250 \bmod p,$$

toraj $a_0 = 1$ in $\log_{71} 210 \equiv 1 u \pmod 2$.

Modul 5: $\gamma_0 = 1$,

$$\gamma_1 \equiv \alpha^{250/5} \equiv 20 \mod p$$

in

$$\beta^{250/5} \equiv 149 \mod p,$$

torej $a_0 = 2$. ...
$a_1 = 4 = \log_{20} 113$ in $a_2 = 2 = \log_{20} 149$.

$\log_{71} 210 \equiv 2 + 4 \cdot 5 + 2 \cdot 5^2 \equiv 72 \pmod{125}$.

Končno na metoda KO da $\log_{71} 210 = 197$.

Metoda index calculus

$GF(23)^*$ z generatorem 5: izberi bazo 'majhnih' faktorjev: $B = \{-1, 2, 3\}$ in sestavi tabelo njihovih logaritmov:

elt	-1	2	3
log	11	2	16

Iščemo logaritem elementa β (Las Vegas).
Poišči 'gladko' potenco elementa β,
tj. β^x, ki se da razstaviti na faktorje iz B.

Izračunaj log(13): $13^2 = 161 = 2^3 \iff$
$\log 13^2 = \log 2^3 \iff 2 \log 13 \equiv 3 \log 2 \iff$
$2 \log 13 \equiv 6 \pmod{22}$
Sledi $\log 13 \equiv 3$ ali $14 \pmod{22}$
Preverimo $\log 13 = 14$.

Izračunaj log(14):
$14^3 = 2^3 7^3 = 2^3 \cdot 21 = 2^3 \cdot (-2) = -2^4$.
$3 \log 14 = \log(-2^4) = \log(-1) + \log 2^4 = 11 + 4 \cdot 2 = 19$,
$\log 14 = \frac{19}{3} = 19 \cdot (-7) = (-3)(-7) = 21$.

Izračunaj log(15):
$15^3 = 3^3 \cdot 5^3 = 3^3 \cdot 2 \cdot 5 = (-1) \cdot 2 \cdot 3$,
$3 \log 15 = \log(-1) + \log 2 + \log 3 = 11 + 2 + 16 = 29 = 7$,
$\log 15 = \frac{7}{3} = 7(-7) = -49 = -5 = 17$.

Izračunaj log(7):
$7^3 = 49 \cdot 7 = 3 \cdot 7 = 21 = (-1) \cdot 2$,
$3 \log 7 = \log(-1) + \log 2 = 11 + 2 = 13$,
$\log 7 = \frac{13}{3} = 13 \cdot (-7) = 63 = -3 = 19$.

Še en primer: $GF(89)^*$ z gen. 3.

tabela logaritmov:

elt	-1	2	3	5
log	44	16	1	70

Izračunaj log(7):
$7^3 = 76 = 2^2 \cdot 19$, $7^5 = 3 \cdot 5^2$,
$5 \log 7 = \log 3 + 2 \log 5 = 1 + 2 \cdot 70 = 141 = 53$,
$\log 7 = \frac{53}{5} = 53 \cdot (-35) = 81$.

Izračunaj log(53):
$53^3 = 3 \cdot 23$, $53^5 = 2^2 \cdot 17$, $53^7 = 2 \cdot 3^2$,
$7 \log 53 = \log 2 + 2 \log 3 = 16 + 2 = 8$,
$\log 53 = \frac{18}{7} = 18 \cdot (-25) = 78$.

Metoda index calculus (splošno)

1. Izberi bazo faktorjev $\mathcal{B} = \{p_1, \ldots, p_t\}$, tako da se da dovolj veliko število elementov grupe G dovolj hitro razstaviti v $\mathcal{B}$.

2. Poišči $t + 10$ lineranih zvez z logaritimi elementov iz $\mathcal{B}$: izberi naključno število $k \in \{1, \ldots, n\}$, izračunaj α^k in ga poskusi zapisati kot $\alpha^k = \Pi_{i=1}^t p_i^{c_i}$.

3. Sestavi tabelo logaritmov elementov iz $\mathcal{B}$.

4. Izberi naključno število $k \in \{1, \ldots, n\}$, izračunaj $\beta\alpha^k$ in ga poskusi zapisati kot

$$\beta\alpha^k = \Pi_{i=1}^t p_i^{d_i}.$$

Končno dobimo

$$\log_\alpha \beta = (\sum_{i=1}^{t} d_i \log_\alpha p_i - k) \mod n.$$

Primer končnega obsega: $GF(2^4)$

Izberimo $f(x) = 1 + x + x^4 \in GF(2)[x]$. Naj bo $a_0 + a_1 x + a_2 x^2 + a_3 x^3 = (a_0, a_1, a_2, a_3)$. Elementi obsega $GF(2^4)$ so:

(1000)	(1100)	(1010)	(1111)
(0100)	(0110)	(0101)	(1011)
(0010)	(0011)	(1110)	(1001)
(0001)	(1101)	(0111)	(0000)

Definirajmo operaciji '+' in '×' v $GF(p^n)$:

$(a_0, \ldots, a_{n-1}) + (b_0, \ldots, b_{n-1}) = (c_0, \ldots, c_{n-1})$

kjer je $c_i = a_i + b_i \pmod p$.

$(a_0, \ldots, a_{n-1}) \times (b_0, \ldots, b_{n-1}) = (r_0, \ldots, r_{n-1})$

kjer je $(r_0, \ldots, r_{n-1})$ ostanek produkta $(a_0, \ldots, a_{n-1}) \times (b_0, \ldots, b_{n-1})$ pri deljenju z nerazcepnim polinomom $f(x)$ stopnje n.

Primer: $(1011) + (1001) = (0010)$.

$(1011) \times (1001)$
$= (1 + x^2 + x^3)(1 + x^3) = 1 + x + x^5 + x^6$
$= (x^4 + x + 1)(x^2 + x) + (1 + x + x^2 + x^3)$
$= (1111)$.

$GF(2^4)^*$

Izberimo $f(x) = 1 + x + x^4$. $GF(2^4)^*$ je lahko generiran z enim elementom $\alpha = x$.

$\alpha_0 = (1000)$	$\alpha_8 = (1010)$
$\alpha_1 = (0100)$	$\alpha_9 = (0101)$
$\alpha_2 = (0010)$	$\alpha_{10} = (1110)$
$\alpha_3 = (0001)$	$\alpha_{11} = (0111)$
$\alpha_4 = (1100)$	$\alpha_{12} = (1111)$
$\alpha_5 = (0110)$	$\alpha_{13} = (1011)$
$\alpha_6 = (0011)$	$\alpha_{14} = (1001)$
$\alpha_7 = (1101)$	$\alpha_{15} = \alpha^0 = 1$

Log tabela

log	elt		log	elt
0	(1000)		8	(1010)
1	(0100)		9	(0101)
2	(0010)		10	(1110)
3	(0001)		11	(0111)
4	(1100)		12	(1111)
5	(0110)		13	(1011)
6	(0011)		14	(1001)
7	(1101)			

Zech log tabela

$1 + \alpha^i = \alpha^{z(i)}$				
i	$z(i)$		i	$z(i)$
∞	0		7	9
0	∞		8	2
1	4		9	7
2	8		10	5
3	14		11	12
4	1		12	11
5	10		13	6
6	13		14	3

Grupa na eliptični krivulji

Za kriptografijo sta jo leta 1985 prva predlagala Neal Koblitz in Victor Miller.

Eliptična krivulja E nad obsegom $GF(p)$ je def. z Weierstrassovo enačbo:

$$y^2 = x^3 + ax + b$$

kjer sta $a, b \in \mathbb{Z}_p$ in $4a^3 + 27b^2 \not\equiv 0 \pmod p$
($GF(2^m)$: $y^2 + xy = x^3 + ax^2 + b$)

Množica $E(\mathbb{Z}_p)$ je sestavljena iz točk (x, y), $x, y \in \mathbb{Z}_p$, katere ustrezajo zgornji enačbi, vključno s točko neskončno $\mathcal{O}$.

THEOREM (Hasse).

$$p + 1 - 2\sqrt{p} \leq |E| \leq p + 1 + 2\sqrt{p}$$

Schoofov algoritem izračuna $|E|$ v $O((\log p)^8)$ bitnih operacijah.

Grupa E je izomorfna $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$, kjer $n_2 | n_1$ in $n_2 | (p-1)$, tako da lahko najdemo ciklično podgrupo $\mathbb{Z}_{n_1}$, ki jo uporabimo za ElGamalov kriptosistem.

Zaenkrat ne znamo uporabiti metodo index calculus pri diskretnem logaritmu na eliptični grupi (razen če ni eliptična krivulja supersingularna). Zato si lahko izberemo eliptično krivuljo s ciklično podgrupo velikosti (samo) okoli 2^{160}.

Pravilo za seštevanje:

1. $P + \mathcal{O} = \mathcal{O} + P = P$ za vsak $P \in E(\mathbb{Z}_p)$.
2. Če je $P = (x, y) \in E(\mathbb{Z}_p)$, potem je $(x, -y) =: -P \in E(\mathbb{Z}_p)$ in $P + (-P) = \mathcal{O}$.

3. $P = (x_1, y_1) \in E(\mathbb{Z}_p)$ in $Q = (x_2, y_2) \in E(\mathbb{Z}_p)$, kjer $P \neq -Q$. Potem je $P + Q = (x_3, y_3)$, kjer je $x_3 = \lambda^2 - x_1 - x_2$, $y_3 = \lambda(x_1 - x_3) - y_1$, in

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

Primer: EC nad $GF(2^4)$

- Naj bo $GF(2^4)$ generiran s korenom $\alpha = x$ nerazcepnega polinoma $f(x) = 1 + x + x^4$.
- $E_1: \quad y^2 + xy = x^3 + \alpha^4 x^2 + 1$. Velja: $j(E_1) \neq 0$.
- $E_1(GF(2^4))$ $= \{(x, y) : y^2 + xy = x^3 + \alpha^4 x^2 + 1\} \cup \{\mathcal{O}\}$.
- $E_1(GF(2^4))$ tvori "grupo" za seštevanje, z $\mathcal{O}$ kot identiteto.

Rešitve enačbe:

$$y^2 + xy = x^3 + \alpha^4 x^2 + 1 \quad \text{nad GF}(2^4)$$

$(0, 1)$	
$(1, \alpha^6)$	$(1, \alpha^{13})$
(α^3, α^8)	(α^3, α^{13})
(α^5, α^3)	(α^5, α^{11})
(α^6, α^8)	(α^6, α^{14})
(α^9, α^{10})	(α^9, α^{13})
(α^{10}, α^1)	(α^{10}, α^8)
$(\alpha^{12}, 0)$	$(\alpha^{12}, \alpha^{12})$

Primer seštevanja v $E_1(GF(2^4))$:

Let $P_1 = (\alpha^6, \alpha^8)$, $P_2 = (\alpha^3, \alpha^{13})$.

- $P_1 + P_2 = (x_3, y_3)$.

$$\begin{aligned} x_3 &= (\frac{\alpha^8 + \alpha^{13}}{\alpha^6 + \alpha^3})^2 + \frac{\alpha^8 + \alpha^{13}}{\alpha^6 + \alpha^3} + \alpha^6 + \alpha^3 + \alpha^4 \\ &= (\frac{\alpha^3}{\alpha^2})^2 + \frac{\alpha^3}{\alpha^2} + \alpha^2 + \alpha^4 = 1 \end{aligned}$$

$$\begin{aligned} y_3 &= (\frac{\alpha^8 + \alpha^{13}}{\alpha^6 + \alpha^3})(\alpha^6 + 1) + 1 + \alpha^8 \\ &= (\frac{\alpha^3}{\alpha^2})\alpha^{13} + \alpha^2 = \alpha^{13} \end{aligned}$$

- $2P_1 = (x_3, y_3)$.

$$\begin{aligned} x_3 &= (\alpha^6)^2 + \frac{1}{(\alpha^6)^2} \\ &= \alpha^{12} + \alpha^3 = \alpha^{10} \end{aligned}$$

$$\begin{aligned} y_3 &= (\alpha^6)^2 + (\alpha^6 + \frac{\alpha^8}{\alpha^6})\alpha^{10} + \alpha^{10} \\ &= \alpha^3 + (\alpha^6 + \alpha^2)\alpha^{10} = \alpha^8 \end{aligned}$$

Še en primer EC nad $GF(2^4)$

- Naj bo $GF(2^4)$ generiran s korenom $\alpha = x$ nerazcepnega polinoma $f(x) = 1 + x + x^4$.
- $E_2: \quad y^2 + \alpha^6 y = x^3 + \alpha^3 x + 1$. Velja $j(E_2) = 0$.
- $E_2(GF(2^4))$ $= \{(x, y) : y^2 + \alpha^6 y = x^3 + \alpha^3 x + 1\} \cup \{\mathcal{O}\}$.
- $E_2(GF(2^4))$ tvori "grupo" za seštevanje z $\mathcal{O}$ kot identiteto.

Rešitve enačbe

$$y^2 + \alpha^6 y = x^3 + \alpha^3 x + 1$$

nad $GF(2^4)$.

Ta enačba ima samo 8 rešitev:

(α^2, α^8)	(α^2, α^{14})
$(\alpha^{10}, 1)$	$(\alpha^{10}, \alpha^{13})$
$(\alpha^{11}, 0)$	(α^{11}, α^6)
(α^{13}, α^5)	(α^{13}, α^9)

Primer: EC nad $GF(23)$

- Naj bo $p = 23$.
- $y^2 = x^3 + x + 1$, (i.e $a = 1$, $b = 1$).
  Velja: $27a^3 + 16b^2 = 3 \cdot 1^3 + 16 \cdot 1^3 = 19 \neq 0$ v $GF(23)$
- $E_3(GF(23)) = \{(x,y) : y^2 = x^3 + x + 1\} \cup \{\mathcal{O}\}$.
- $E_3(GF(23))$ tvori "grupo" za seštevanje z $\mathcal{O}$ kot identiteto.

Rešitve enačbe

$$y^2 = x^3 + x + 1.$$

nad $\mathbb{Z}_{23}$.

(0, 1)	(6, 4)	(-11,-4)
(0,-1)	(6,-4)	(-10, 7)
(1, 7)	(7, 11)	(-10,-7)
(1,-7)	(7,-11)	(-6, 3)
(3, 10)	(9, 7)	(-6,-3)
(3,-10)	(9,-7)	(-5, 3)
(4, 0)	(11, 3)	(-5,-3)
(5, 4)	(11,-3)	(-4, 5)
(5,-4)	(-11,4)	(-4,-5)

Primer seštevanja na $E_3(GF(23))$

1. $P_1 = (3,10)$, $P_2 = (9,7)$,
   $P_1 + P_2 = (x_3, y_3)$.

   $\lambda = \frac{7-10}{9-3} = \frac{-3}{6} = \frac{-1}{2} = 11 \in \mathbb{Z}_{23}$.

   $x_3 = 11^2 - 3 - 9 = 6 - 3 - 9 = -6$,
   $y_3 = 11(3 - (-6)) - 10 = 11(9) - 10$
   $= 89 = 20 = -3$.
   Sledi $P_1 + P_2 = (-6, -3)$.

2. $P_1 = (3,10)$, $2P_1 = (x_3, y_3)$,

   $\lambda = \frac{3(3^2)+1}{20} = \frac{5}{20} = \frac{1}{4} = 6$.

   $x_3 = 6^2 - 6 = 30 = 7$,
   $y_3 = 6(3 - 7) - 10 = -24 - 10 = -11$.
   Sledi $2P_1 = (7, -11)$.

$P = (0,1)$ je generator

P=(0, 1)	
$2P$=(6,-4)	$15P$=(9, 7)
$3P$=(3,-10)	$16P$=(-6,3)
$4P$=(-10,-7)	$17P$=(1,7)
$5P$=(-5,3)	$18P$=(12,-4)
$6P$=(7,11)	$19P$=(-4,5)
$7P$=(11,3)	$20P$=(5,4)
$8P$=(5,-4)	$21P$=(11,-3)
$9P$=(-4,-5)	$22P$=(7 -11)
$10P$ =(12,4)	$23P$=(-5,-3)
$11P$=(1,-7)	$24P$=(-10,7)
$12P$=(-6,-3)	$25P$=(3,10)
$13P$=(9,-7)	$26P$=(6,4)
$14P$=(4,0)	$27P$=(0,-1)

Log – antilog tabela

log	elt	log	elt
0	$\mathcal{O}$	14	(4,0)
1	(0,1)	15	(9,7)
2	(6,-4)	16	(-6,3)
3	(3,-10)	17	(1,7)
4	(-10,-7)	18	(-11,-4)
5	(-5,3)	19	(-4,5)
6	(7,11)	20	(5,4)
7	(11,3)	21	(11,-3)
8	(5,-4)	22	(7,-11)
9	(-4,-5)	23	(-5,-3)
10	(-11,4)	24	(-10,7)
11	(1,-7)	25	(3,10)
12	(-6,-3)	26	(6,4)
13	(9,-7)	27	(0,-1)

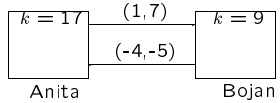
Log – antilog tabela

elt	log	elt	log
$\mathcal{O}$	0	(9,7)	15
(0,1)	1	(9,-7)	13
(0,-1)	27	(11,3)	7
(1,7)	17	(11,-3)	21
(1,-7)	11	(-11,4)	10
(3,10)	25	(-11,-4)	18
(3,-10)	3	(-10,7)	24
(4,0)	14	(-10,-7)	4
(5,4)	20	(-6,3)	16
(5,-4)	8	(-6,-3)	12
(6,4)	26	(-5,3)	5
(6,-4)	2	(-5,-3)	23
(7,11)	6	(-4,5)	19
(7,-11)	22	(-4,-5)	9

Diffie–Hellmanov protocol nad $E(GF(23))$

Javni parametri:

$$y^2 = x^3 + x + 1$$
$$P = (0,1)$$



- Anita izračuna $17P = (1,7)$
- Bojan izračuna $9P = (-4,-5)$
- Anita izračuna $17(-4,-5) = (6,4)$
- Bojan izračuna $9(1,7) = (6,4)$.

Anita in Bojan imata skupno točko $(6,4)$.

Računanje logaritmov

Izračunaj $\log_P(9,7)$**.**

Izračunaj naslednjo tabelo:

elt	(0,1)	(7,11)	(-6,-3)	(12,-4)	(-10,7)
log	1	6	12	18	24

Če je $k = \log_P(9,7)$, potem velja $kP = (9,7)$.

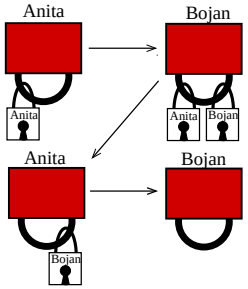
- Računaj
  $(9,7) + P$, $(9,7) + 2P$, $(9,7) + 3P, \ldots$
  vse dokler ne dobiš element iz tabele.
- Dobimo: $(9,7) + 3P = (12,-4)$.
- Iz tabele preberemo $(12,-4) = 18P$
- Sledi $(9,7) + 3P = 18P$
  oziroma $(9,7) = 15P$, torej $k = 15$

- Če je $|E(GF(q))| = n$ lahko posplošimo metodo za $E(GF(23))$ na naslednji način:
  - naredi tabelo (i, iP) velikosti $\sqrt{n}$,
  - za iskanje logaritma elementa v tej tabeli potrebujemo največ $\sqrt{n}$ seštevanj točk.
- Če je $q \approx 10^{40}$, potem je $|E(GF(q))| \approx 10^{40}$ in ima tabela 10^{20} vrstic.
  To je očitno popolnoma nedosegljivo.

Albrecht Beutelspacher, **Cryptology**, MAA, 1994 (pri nas v CTK 206835 INF-A)

D. Kahn, **The Codebreakers**
(The Story of Secret Writing),
hrvaški prevod: (K. and M. Miles),
Šifranti protiv špijuna,
Centar za informacije i Publicitet, Zagreb 1979.
(429+288+451+325=1493 strani).

Massey-Omura shema



Nekaj lažjih nalog:

1. Koliko množenj potrebujemo, da izračunamo m^d?

2. Prepričaj se, da pri RSA uporabimo samo Fermatovo kongruenco.

3. Pokaži, da $p|\binom{p}{i}$, za $1 < i < p$.

4. Naj bo p praštevilo, potem za poljubni števili a in b velja:

$$(a+b)^p \bmod p = a^p + b^p \bmod p.$$

5. Naj bo p praštevilo, potem za poljubno število m velja $m^p \bmod p = m$.

Prihodnjič:

T. Klobučar prične s 6. poglavjem:

- Digitalni podpisi

Do naslednič:

- pričnite brati 6. poglavje (str. 202-213)

- rešujte naloge 5. poglavja

Stinsonovega učbenika
Cryptography, Theory and Practice