RSA

i) Izberemo praštevili p, q

ii) $n = p \cdot q$

iii) $\varphi(n) = (p-1) \cdot (q-1)$

iv) Izberemo e, $1 < e < \varphi(n)$, da je $\gcd(e, \varphi(n)) = 1$

v) Izračunamo $d = e^{-1} \bmod \varphi(n)$

vi) Objavimo javni ključ $(n, e) = (p \cdot q, e)$

vii) Shranimo zasebni ključ $(n, d) = (p \cdot q, d)$

Šifriranje: $c = m^e \bmod n$

Dešifriranje: $m = c^d \bmod n \quad (= (m^e)^d \bmod n)$

ALGORITEM KVADRIRAJ IN MNOŽI

$a \in \mathbb{N}$
$m = b_{k-1} b_{k-2} \cdots b_1 b_0$
$n \in \mathbb{N}$

$a^m \bmod n$:

$p = 1$

$\forall i = 0, 1, \ldots, k-1$:

$b_i = 1 \Rightarrow p = p \cdot a \bmod n$

$a = a^2 \bmod n$

$\rightarrow p =: a^m \bmod a$

---

2) Dani sta praštevili $p = 11$ in $q = 17$ ter kodirni eksponent $e = 9$.

a) Preverite, da je $(p \cdot q, e)$ veljavni javni ključ za RSA.

b) Izračunajte še ustrezni dekodirni eksponent d.

c) Z javnim ključem $(p \cdot q, e)$ zašifrirajte besedilo 107. Za potenciranje uporabite algoritem kvadriraj in množi.

d) Z zasebnim ključem $(p \cdot q, d)$ dešifrirajte kriptogram 6.

a) Preveriti moramo, da je $\gcd(e, \varphi(n)) = 1$.

$n = p \cdot q = 11 \cdot 17 = 187$

$\varphi(n) = (p-1)(q-1) = 10 \cdot 16 = 160 = 2^5 \cdot 5$

$\Rightarrow 9$ je tuj z 160.

b) $e \cdot d \equiv 1 \bmod \varphi(n)$

$$160 = 17 \cdot 9 + 7$$
$$9 = 1 \cdot 7 + 2$$
$$7 = 3 \cdot 2 + 1$$

$$\Rightarrow 1 = 7 - 3 \cdot 2 = 7 - 3(9-7) = 7(1+3) - 3 \cdot 9$$

$$= (160 - 17 \cdot 9) \cdot 4 - 3 \cdot 9 = 160 \cdot 4 + 9(-17 \cdot 4 - 3)$$

$$= 160 \cdot 4 + 9 \cdot (-71)$$

$$= 160 \cdot 4 + 9 \cdot (160 - 71)$$

$$= 160 \cdot 4 + 9 \cdot 89$$

$$\Rightarrow d = 89$$

c) $c = m^e \bmod n = 107^9 \bmod 178$

$9 = (1001)_2$

$a = 107$
$m = 9$
$n = 178$

$p = 1$

$b_0 = 1 \Rightarrow p = 1 \cdot 107 \bmod 187 = 107$

$a = a^2 \bmod n = 107^2 \bmod 187 = 42$

$b_1 = 0 \Rightarrow p = 107$

$a = a^2 \bmod n = 42^2 \bmod 187 = 81$

$b_2 = 0 \Rightarrow p = 107$

$a = a^2 \bmod n = 81^2 \bmod 187 = 16$

$b_3 = 1 \Rightarrow p = 107 \cdot 16 \bmod 187 = 29$

$\Rightarrow 107^9 \equiv 29 \bmod 187$

d) $m = c^d \bmod n = 6^8 \bmod 187$

Podobno ...

---

3) Alenka ima javni ključ (n, e_1), Boris pa javni ključ (n, e_2), pri čemer je $\gcd(e_1, e_2) = 1$. Cene sporočilo b zašifrira z obema javnima ključema in kriptograma pošlje Alenki oziroma Borisu. Eva prestreže oba kriptograma $c_1 = b^{e_1} \bmod n$ in $c_2 = b^{e_2} \bmod n$.

a) Pokažite, kako lahko Eva dešifrira kriptogram, brez da faktorizira n.

b) Napad pokažite na primeru $n = 55$, $e_1 = 3$, $e_2 = 7$, $c_1 = 8$ in $c_2 = 18$.

a) $c_1 = b^{e_1} \bmod n$
$c_2 = b^{e_2} \bmod n$

$\gcd(e_1, e_2) = 1 \Rightarrow \exists \alpha, \beta : e_1\alpha + e_2\beta = 1 \qquad (v \mathbb{Z})$

$c_1^{\alpha} \cdot c_2^{\beta} = (b^{e_1})^{\alpha} \cdot (b^{e_2})^{\beta} = b^{e_1\alpha} \cdot b^{e_2\beta} = b^{e_1\alpha + e_2\beta} = b \bmod n$

b) $3\alpha + 7\beta = 1$

$\Rightarrow \beta = 1, \alpha = -2$

$8^{-2} \cdot 19^1 \bmod 55 = 7^2 \cdot 19^1 \bmod 55 = 2 \bmod 55$

---

4) Recimo, da sistem uporablja RSA. Napadalec želi dešifrirati kriptogram c, da bi pridobil ustrezno besedilo b. Predpostavimo, da sistem zlahka dešifrira poljubna izbrana zašifrirana sporočila, razen samega kriptograma c. Pokažite, da je možen napad z izbranim šifriranim besedilom.

$c = b^e \bmod n$

i) Zašifriramo $c_r = r^e \bmod n$

ii) Izračunamo $c' = c \cdot c_r$

iii) Dešifriramo $b' = (c')^d \bmod n$

$b' = (c')^d \bmod n$

$= (c \cdot c_r)^d \bmod n$

$= (b^e \cdot r^e)^d \bmod n$

$= (b \cdot r)^{e \cdot d} \bmod n$

$= (b \cdot r)^{1 + k\varphi(n)} \bmod n$

$= (b \cdot r) \cdot \underbrace{(b \cdot r)^{k\varphi(n)}}_{1} \bmod n$

$= b \cdot r \bmod n$

$\Rightarrow b = b' \cdot r^{-1} \bmod n \quad , \quad \gcd(r, n) = 1$

KITAJSKI IZREK O OSTANKIH (CRT)

$0 < x \leq N = n_1 n_2 \cdots n_k$

$x \equiv a_1 \mod n_1$
$x \equiv a_2 \mod n_2$
$\vdots$
$x \equiv a_k \mod n_k$

$\Rightarrow \exists! \, x \in \{0, 1, \ldots, N-1\}$:

$$x \equiv \sum_{i=1}^{k} a_i M_i N_i \mod N$$

$N_i = \frac{N}{n_i}$

$M_i N_i = 1 \mod n_i$

---

1) Naj bodo n_1, n_2, n_3 paroma tuji moduli za RSA kriptosistem in $e = 3$. Naj bo $c_i = b^e \mod n_i$, $i = 1,2,3$, torej isto sporočilo zašifriramo s tremi različnimi javnimi ključi.

a) Poiščite besedilo b.

Namig: Uporabite kitajski izrek o ostankih

b) Napad ilustrirajte na primeru $n_1 = 55$, $n_2 = 391$, $n_3 = 1189$, $c_1 = 6$, $c_2 = 105$, $c_3 = 1148$.

a) $c_1 \equiv b^3 \mod n_1$
$c_2 \equiv b^3 \mod n_2$
$c_3 \equiv b^3 \mod n_3$

$\Leftrightarrow$

$b^3 \equiv c_1 \mod n_1$
$b^3 \equiv c_2 \mod n_2$
$b^3 \equiv c_3 \mod n_3$

$\Rightarrow b^3 \equiv x \mod N$

$b < n_1, n_2, n_3$

$\Rightarrow b^3 < n_1 n_2 n_3 = N$

$\Rightarrow b^3 = x$

$\Rightarrow b = \sqrt[3]{x}$

b) $b^3 \equiv 6 \mod 55$
$b^3 \equiv 105 \mod 391$
$b^3 \equiv 1148 \mod 1189$

$N_1 = \frac{N}{n_1} = \frac{55 \cdot 391 \cdot 1189}{55} = 464899$
$N_2 = \frac{N}{n_2} = \frac{55 \cdot 391 \cdot 1189}{391} = 65395$
$N_3 = \frac{N}{n_3} = \frac{55 \cdot 391 \cdot 1189}{1189} = 21505$

$M_1 = N_1^{-1} \vee \mathbb{Z}_{55}^* = 24$
$M_2 = N_2^{-1} \vee \mathbb{Z}_{391}^* = 4$
$M_3 = N_3^{-1} \vee \mathbb{Z}_{1189}^* = 658$

$\Rightarrow x \equiv 6 \cdot 464899 \cdot 24 + 105 \cdot 65395 \cdot 4 + 1148 \cdot 21505 \cdot 658$

$\equiv 68921 \mod (55 \cdot 391 \cdot 1189)$

$\Rightarrow b = \sqrt[3]{68921} = 41$

---

2) Naj bo $(n = p \cdot q, e)$ javni ključ za RSA. Koliko besedil iz $\mathbb{Z}_n$ se pri šifriranju s ključem (n, e) ne spremeni?

Koliko je to za $n = 85$ in $e = 33$?

Namig: CRT $\Rightarrow (\mathbb{Z}_n, +, \cdot) \cong (\mathbb{Z}_p, +, \cdot) \times (\mathbb{Z}_q, +, \cdot)$

$x^e \equiv x \mod n$

$\Rightarrow x_1^e \equiv x_1 \mod p$ in $x_2^e \equiv x_2 \mod q$

$x_1^e \equiv x_1 \mod p$
$x_1^e - x_1 \equiv 0 \mod p$
$x_1(x_1^{e-1} - 1) \equiv 0 \mod p$

$\Rightarrow x_1 = 0$ ali $x_1^{e-1} \equiv 1 \mod p$

$x_1^{e-1} \equiv 1 \mod p$
$(g^{y_1})^{e-1} \equiv 1 \mod p \quad (\mathbb{Z}_p^*)$
$g^{y_1(e-1)} \equiv 1 \mod p$

$\Rightarrow y_1(e-1) \equiv 0 \mod p-1$

$y_1(e-1) = (p-1) \cdot l$

$d = \gcd(e-1, p-1)$

$e-1 = d \cdot a$
$p-1 = d \cdot b$
a, b tuji

$\Rightarrow y_1 \cdot d \cdot a = d \cdot b \cdot l$

$\Rightarrow y_1 \cdot a = b \cdot l$

$\Rightarrow a \mid l$

$\Rightarrow l = a \cdot l'$

$\Rightarrow y_1 \cdot a = b \cdot a \cdot l'$

$\Rightarrow y_1 = b \cdot l'$

$\Rightarrow y_1 = l' \cdot \frac{p-1}{d}$

$y_1 \in \mathbb{Z}_{p-1} = \{0, 1, \dots, p-2\}$

$y_1 = 0, \frac{p-1}{d}, 2 \cdot \frac{p-1}{d}, \dots, (d-1) \cdot \frac{p-1}{d}$

$\Rightarrow$ Obstaja $d = \gcd(e-1, p-1)$ takšnih y_1, da je $y_1(e-1) \equiv 0 \mod p-1$.

$\Rightarrow$ $x_1 : \gcd(e-1, p-1) + 1$
$x_2 : \gcd(e-1, q-1) + 1$

$\Rightarrow x : (\gcd(e-1, p-1) + 1) \cdot (\gcd(e-1, q-1) + 1)$

$n = 85 = 5 \cdot 17$

$x^{33} \equiv x \mod 85$

$\gcd(32, 4) = 4$
$\gcd(32, 16) = 16$

$\Rightarrow (4+1) \cdot (16+1) = 85$

$(p-1) \mid (e-1)$ in $(q-1) \mid (e-1)$

$\Rightarrow$ RSA ne navedi nič!

---

3) Pokažite, da napadalec, ki je pridobil dekodirni ključ d, ki ustreza kodirnemu ključu $e=3$ v RSA kriptosistemu, lahko faktorizira $n=p\cdot q$.

$e \equiv 1 \mod \varphi(n) \Rightarrow ed-1 = k\cdot\varphi(n) \Rightarrow 3d-1 = k\cdot\varphi(n)$

$d < \varphi(n)$
$3d < 3\varphi(n)$
$3d-1 < 3\varphi(n)$
$k\cdot\varphi(n) < 3\varphi(n)$
$k < 3$

$\Rightarrow k=1$ ali $k=2$

$3d-1 \equiv -1 \equiv 2 \mod 3$

$\varphi(n) = (p-1)\cdot(q-1)$

$p \bmod 3$	$q \bmod 3$	$\varphi(n) \bmod 3$
1	1	0
1	2	0
2	1	0
2	2	1

$k=1 \Rightarrow 3d-1 = 1\cdot\varphi(n) \Rightarrow$ ✗

$k=2 \Rightarrow 3d-1 = 2\cdot\varphi(n) \Rightarrow \varphi(n) = \frac{3d-2}{2}$

$\varphi(n) = (p-1)(q-1) = \underbrace{pq}_{=n} - p - q + 1 = n+1-p-q$

$\Rightarrow q = (n+1) - p - \varphi(n)$

$n = p \cdot q$

$n = p \cdot (n+1-p-\varphi(n))$

$p^2 - (n+1-\varphi(n))p + n = 0$

Rešimo enačbo ...

---

4) Uporabljamo kriptosistem RSA: $c = b^e \bmod n$, $n = p \cdot q$. Prestregli smo kriptogram c in pridobili informacijo, da velja $b^{12345} \equiv 1 \bmod n$. Dešifrirajte kriptogram c.

$b^{\varphi(n)} \equiv 1 \bmod n$

$\Psi = 12345$

$e \cdot d \equiv 1 \bmod \Psi$

$\Rightarrow e^d = (b^e)^d = b^{e \cdot d} = b^{k \cdot \Psi + 1} = (\underbrace{b^\Psi}_{=1})^k \cdot b \equiv b \bmod n$

---

5) Naj bo $n = p \cdot q$ in p, q praštevili. Definirajmo $\lambda(n) = \frac{(p-1)\cdot(q-1)}{\gcd(p-1, q-1)}$. Predpostavimo, da smo spremenili RSA na način, da je $ed \equiv 1 \bmod \lambda(n)$.

a) Dokažite, da sta dekodirni in kodirni ključ še vedno inverza v originalnem RSA kriptosistemu.

b) Naj bo $p=3$, $q=5$, $e=7$. Izračunajte d v spremenjenem in originalnem RSA kriptosistemu.

a) $x^{ed} \equiv x \mod n$?

$ed \equiv 1 \mod \lambda(n)$

$ed = k \cdot \lambda(n) + 1$

$x^{\lambda(n)} \mod p = x^{\frac{(p-1)(q-1)}{\gcd(p-1,q-1)}} = (x^{p-1})^{\frac{q-1}{\gcd(p-1,q-1)}} \overset{\text{mali Fermat}}{\equiv} 1 \mod p$

$x^{\lambda(n)} \mod q \equiv 1 \mod q$

CRT $\Rightarrow x^{\lambda(n)} \equiv 1 \mod n$

$\Rightarrow x^{ed} = x^{k \cdot \lambda(n)+1} = (x^{\lambda(n)})^k \cdot x \equiv x \mod n$

b) DN

31.3.

MILLER-RABINOV TEST

Naj bo n liho število in zapišimo $n-1 = 2^s \cdot d$, kjer je d liho število.

Naj bo $a \in \mathbb{Z}$ tuj z n.

- $a^d \equiv 1 \mod n$
- $\exists r \in \{0,1,\dots,r-1\} : a^{2^r \cdot d} \equiv -1 \mod n$

Če ena od teh dveh enakosti velja, potem je p po veliki verjetnosti praštevilo.

Verjetnost, da število ni praštevilo, je vsakič ko opravimo test $\frac{1}{4}$.

Če opravimo k testov, je verjetnost, da število ni praštevilo, enaka $\frac{1}{4^k}$.

1) S pomočjo Miller-Rabinovega testa poiščite 8 bitno praštevilo, oziroma tako 8 bitno število, da boste vsaj 2 verjetnostjo $1-\frac{1}{16}$ prepričani, da je praštevilo.

Iščemo število $n \in [2^7, 2^8)$.

- $n = 231$

  $n-1 = 230 = 2^1 \cdot 115$

  i) $a = 55$

  $\gcd(231, 55) = 11$

- $n = 197$

  $n-1 = 196 = 2^2 \cdot 49$

  i) $a = 98$

  $\gcd(197, 98) = 1$

  $a^d = 98^{49} \equiv 183 \mod 197$

  $a^{2d} = 98^{2 \cdot 49} \equiv -1 \mod 197$

  ii) $a = 113$

  $\gcd(197, 113) = 1$

$$a^d = 113^{49} \equiv 14 \mod 197$$

$$a^{2d} = 113^{2 \cdot 49} \equiv -1 \mod 197$$

$\Rightarrow n = 197$ je praštevilo z verjetnostjo $1 - \frac{1}{16}$

---

2) Naj bo p praštevilo in $(\mathbb{Z}_p^*, \cdot)$ grupa.

a) Recimo, da znamo faktorizirati $p-1$. Kako lahko hitro preverimo, ali je dani element iz $\mathbb{Z}_p^*$ generator grupe? Preverite, če je 2 generator grupe $\mathbb{Z}_{181}^*$.

b) Naj bo α generator grupe $\mathbb{Z}_p^*$. Koliksen je red elementa α^i za $i \in \{1, 2, \dots, p-1\}$. Koliksen je red elementa 2^{10} v $\mathbb{Z}_{181}^*$? Poiscite vse potence 2^i, ki imajo red 10 v $\mathbb{Z}_{181}^*$.

c) Koliksna je verjetnost, da je nakljuno izbran element grupe $\mathbb{Z}_p^*$ generator te grupe? Koliksna je ta verjetnost za $p = 181$?

a) x generator $\mathbb{Z}_p^* \iff \text{red}\, x = p-1$

$$p-1 = p_1^{k_1} p_2^{k_2} \dots p_e^{k_e}$$

x generator $\mathbb{Z}_p^* \iff \forall i : x^{\frac{p-1}{p_i}} \neq 1 \mod p$

$$p = 181 \Rightarrow p-1 = 180 = 2^2 \cdot 3^2 \cdot 5$$

$$2^{\frac{180}{2}} = 180 \neq 1 \mod 181$$
$$2^{\frac{180}{3}} = 48 \neq 1 \mod 181$$
$$2^{\frac{180}{5}} = 59 \neq 1 \mod 181$$

$\Rightarrow$ 2 generator grupe $\mathbb{Z}_{181}^*$

b) $red(\alpha^i) = \frac{p-1}{gcd(i,p-1)}$

$red(2^{10}) = \frac{180}{gcd(10,180)} = 18$

$red(2^i) = \frac{180}{gcd(i,180)} = 10$
$gcd(i,180) = 18$
$gcd(18k, 180) = 18$
$18\, gcd(k,10) = 18$
$gcd(k,10) = 1$

$\Rightarrow k \in \{1,3,7,9\}$

$\Rightarrow 2^{18}, 2^{54}, 2^{126}, 2^{162}$

c) α^i generator $\mathbb{Z}_p^*$ $\Rightarrow gcd(i, p-1) = 1$

$P(\alpha^i \text{ je generator}) = \frac{\varphi(p-1)}{p-1}$

$p = 181$: $P(\alpha^i \text{ je generator}) = \frac{\varphi(180)}{180} = \frac{180 \cdot (1-\frac{1}{2}) \cdot (1-\frac{1}{3}) \cdot (1-\frac{1}{5})}{180} = \frac{4}{15}$

SHANTSOV ALGORITEM

Iščemo $\alpha^x = \beta$

$m = \lceil \sqrt{p-1} \rceil$

velik korak: za vsak $j = 0, 1, \ldots, m-1$ izračunaj in uredi $(j, \alpha^{m \cdot j})$ v L_1

mali korak: za vsak $i = 0, 1, \ldots, m-1$, če je $\beta\alpha^{-i}$ v L_1, izračunaj $x = m \cdot j + i$

vrni X

---

3) Naj bo $(\mathbb{Z}_{31}^*, \cdot)$ grupa.

a) Preverite, ali je 13 generator te grupe.

b) Izračunajte red elementa 3^{10}.

c) S pomočjo Shantsovega algoritma (mali korak - velik korak) izračunajte $\log_{13} 19$.

a) DN

b) DN

c) $p = 31$

$\Rightarrow m = \lceil \sqrt{30} \rceil = 6$

α^{6j}, $j = 0, 1, \ldots, 6$

$\Rightarrow L_1 = \{(0,1), (5,1), (4,2), (3,4), (2,8), (1,16)\}$

$i = 0, 1, \ldots, 6$

$i = 0 \Rightarrow 19 \cdot 13^0 = 19 \notin L_1$

$i = 1 \Rightarrow 19 \cdot 13^{-1} = 11 \notin L_1$

$i = 2 \Rightarrow 19 \cdot 13^{-2} = 8 \in L_1$

$\Rightarrow x = 6 \cdot 2 + 2 = 14$

$\Rightarrow \log_{13} 19 = 14 \text{ v } \mathbb{Z}_{31}^*$

---

4) Naj bo p praštevilo in α generator $\mathbb{Z}_p^*$.

a) Pokažite, da je $\alpha^{\frac{p-1}{2}} \equiv p-1 \mod p$.

b) Naj bo $\beta \equiv \alpha^x \mod p$. Pokažite, kako lahko vgotovimo parnost x iz $\beta^{\frac{p-1}{2}}$, torej, ali je x sodo ali liho število.

a) $x = \alpha^{\frac{p-1}{2}}$

$x^2 = \alpha^{p-1} \equiv 1 \mod p$

$x^2 - 1 \equiv 0 \mod p$

$(x-1)(x+1) \equiv 0 \mod p$

i) $x - 1 \equiv 0 \mod p$

$x \equiv 1 \mod p$

 (ni generator)

ii) $x + 1 \equiv 0 \mod p$

$x \equiv -1 \mod p$

$\alpha^{\frac{p-1}{2}} \equiv p-1 \mod p$

b) $\beta^{\frac{p-1}{2}} = (\alpha^x)^{\frac{p-1}{2}} = (\alpha^{\frac{p-1}{2}})^x = (-1)^x \mod p$

$\beta^{\frac{p-1}{2}} = 1 \Rightarrow x$ sodo

$\beta^{\frac{p-1}{2}} = -1 \Rightarrow$ x liho

DIFFIE-HELLMANOVA IZMENJAVA KLJUČEV

5) Diffie-Hellmanovo izmenjavo ključev čim bolj učinkovito posplošite na 3 udeležence.

p praštevilo
α generator $\mathbb{Z}_p^*$

A izbere a
B izbere b
C izbere c

1. krog:

A pošlje B α^a
B pošlje C α^b
C pošlje A α^c

2. krog:

A pošlje B $(\alpha^c)^a = \alpha^{ac}$
B pošlje C $(\alpha^a)^b = \alpha^{ab}$
C pošlje A $(\alpha^b)^c = \alpha^{bc}$

Nato vsak udeleženec potencira

---

6) Naj bo kriptosistem definiran na naslednji način:

1) Alenka izbere dve veliki praštevili p in q in objavi $n = p \cdot q$. Predpostavimo, da je n zelo težko faktorizirati. Alenka izbere še tri naključna števila $e, r_1, r_2 \in \{1, \dots, n-1\}$ in izračuna $e_1 = e^{r_1(p-1)} \bmod n$ in $e_2 = e^{r_2(q-1)} \bmod n$.

Javni ključ je (n, e_1, e_2), zasebni pa (p, q).

2) Boris, ki želi poslati sporočilo b, izbere dve naključni števili $s_1, s_2 \in \{1, \dots, n-1\}$ in izračuna $c_1 = b \cdot e_1^{s_1} \bmod n$ in $c_2 = b \cdot e_2^{s_2} \bmod n$. Nato Boris pošlje Alenki (c_1, c_2).

3) Alenka uporabi kitajski izrek o ostankih in z njim izračuna $x \equiv c_1 \bmod p$, $x \equiv c_2 \bmod q$.

a) Pokažite, da je Alenkina rešitev x enaka Borisovem sporočilu b.

b) Razložite, zakaj ta kriptosistem ni varen.

a) Hočemo pokazati $x \equiv b \bmod p$ in $x \equiv b \bmod q$.

Potem po CRT sledi $x \equiv b \bmod n$.

$$x = c_1 \bmod p$$

$$= (b e_1^{s_1} \bmod n) \bmod p$$

$$= (b e^{r_1 s_1 (p-1)} \bmod n) \bmod p$$

$$= b e^{r_1 s_1 (p-1)} \bmod p$$

$$= b \cdot (\underbrace{e^{p-1}}_{1})^{r_1 s_1} \bmod p$$

$$= b \bmod p$$

Podobno dobimo $x = b \bmod q$.

Torej po CRT velja $x \equiv b \bmod n$.

b) $e_1 = e^{\varphi(n)(p-1)} \bmod p = 1 \bmod p$

$\Rightarrow p \mid (e_1 - 1)$

$\gcd(e_1 - 1, n)$ vsebuje vsaj p

$e_1 \bmod q$

i) $e_1 \equiv 1 \bmod q$

$\Rightarrow \gcd(e_1 - 1, n) = n$

$\Rightarrow c_1 = b \bmod n$

$\Rightarrow$ Napadalec dobi sporočilo

ii) $e_1 \not\equiv 1 \bmod q$

$\Rightarrow \gcd(e_1 - 1, n) = p$

$\Rightarrow$ Napadalec lahko faktorizira n

$\Rightarrow$ Napadalec dobi zasebni ključ

ELGAMALOV KRIPTOSISTEM

p praštevilo
α generator grupe $\mathbb{Z}_p^+$

$B = \alpha^b \bmod p$

Javni ključ: (p, α, B)
Zasebni ključ: (p, α, b)

Šifriranje:

Izberemo naključen $0 < a < p-1$.

$c = (A, y) = (\alpha^a, B^a \cdot x) \mod p$

Dešifriranje:

$x = y \cdot A^{-b}$

---

1) Predpostavimo, da sistem uporablja Elgamalov kriptosistem. Napadalec želi dešifrirati kriptogram $c = (A, y)$, ki ustreza neznanemu sporočilu x. Napadalec ima možnost, da sistemu pošlje poljuben drug kriptogram in prejme njegovo dešifriranje. Pokaži, da lahko napadalec zlorabi to lastnost in določi sporočilo x, ne da bi poznal zaseboni ključ.

Elgamalov sistem je multiplikativno homomorfen:

$c_1 = (A_1, y_1) = (\alpha^{a_1}, B^{a_1} x_1) \mod p$
$c_2 = (A_2, y_2) = (\alpha^{a_2}, B^{a_2} x_2) \mod p$

$\Rightarrow A_1 A_2 = \alpha^{a_1} \alpha^{a_2} = \alpha^{a_1 + a_2} \mod p$
$y_1 y_2 = B^{a_1} x_1 B^{a_2} x_2 = B^{a_1 + a_2} x_1 x_2 \mod p$

$\Rightarrow c = (\alpha^{a_1 + a_2}, B^{a_1 + a_2} x_1 x_2) = c_1 \cdot c_2$

Da to zlorabimo, izberemo $x_1 = 2$ (ker ima 2 gotovo inverz) in izračunamo $c_1 = (A_1, y_1) = (\alpha^{a_1}, B^{a_1} x_1) \mod p$.

Vemo, da je $c = (A, y) = (\alpha^a, B^a x)$.

Torej je $c \cdot c_1 = (A A_1, y y_1)$ veljaven kriptogram, ki ga lahko pošljemo sistemu, da ga dešifrira.

$\Rightarrow \underbrace{x \cdot x_1}_{x'} = 2x \mod p$

$\Rightarrow x = 2^{-1} x' \mod p$

LWE

$Ax + e = y$

---

2) Imamo problem LWE $Ax+e=y$ nad $\mathbb{Z}_{13}$, kjer so:

- $A = \begin{bmatrix} 8 & 3 \\ 4 & 7 \\ 0 & 6 \end{bmatrix}$ znana
- x neznani iskani vektor
- e majhen naključen šum, izbran iz $\{-1, 0, 1\}$
- $y = \begin{bmatrix} 4 \\ 0 \\ 11 \end{bmatrix}$ rezultat z napako

Kako dobro rešitev dobimo z Gaussovo eliminacijo?

$v_1' = v_1 \cdot 8^{-1} = v_1 \cdot 5$ $\quad$ $v_2' = v_2 - 4 \cdot v_1$

$$\left[\begin{array}{cc|c} 8 & 3 & 4 \\ 4 & 7 & 0 \\ 0 & 6 & 11 \end{array}\right] \sim \left[\begin{array}{cc|c} 1 & 2 & 7 \\ 4 & 7 & 0 \\ 0 & 6 & 11 \end{array}\right] \sim \left[\begin{array}{cc|c} 1 & 2 & 7 \\ 0 & 12 & 11 \\ 0 & 6 & 11 \end{array}\right] \sim *$$

$x = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$

$$8x_1 + 3x_2 = 4 \mod 13$$
$$4x_1 + 7x_2 = 0 \mod 13$$
$$0x_1 + 6x_2 = 11 \mod 13$$

$v_2' = v_2 \cdot 12^{-1} = v_2 \cdot 12$ $\quad$ $v_3' = v_3 - 6v_2$

$$* \sim \left[\begin{array}{cc|c} 1 & 2 & 7 \\ 0 & 1 & 2 \\ 0 & 6 & 11 \end{array}\right] \sim \left[\begin{array}{cc|c} 1 & 2 & 7 \\ 0 & 1 & 2 \\ 0 & 0 & 12 \end{array}\right]$$

$\Rightarrow 0 \equiv 12 \mod 13$

$\Rightarrow$ Gaussova eliminacija ne pomaga!

Slučajno smo v prvih dveh vrsticah dobili ok enačbe. To se je zgodilo, ker je šum le na tretji komponenti. V splošnem se to ne dogaja.

Recimo, da vemo, da je $x = \begin{bmatrix} 3 \\ 2 \end{bmatrix}$ rešitev.

Poglejmo, kje smo dobili napako:

$$Ax = \begin{bmatrix} 8 & 3 \\ 4 & 7 \\ 0 & 6 \end{bmatrix} \begin{bmatrix} 3 \\ 2 \end{bmatrix} = \begin{bmatrix} 30 \\ 26 \\ 12 \end{bmatrix} \mod 13 = \begin{bmatrix} 4 \\ 0 \\ 12 \end{bmatrix} \mod 13$$

$$\Rightarrow e = y - Ax = \begin{bmatrix} 4 \\ 0 \\ 11 \end{bmatrix} - \begin{bmatrix} 4 \\ 0 \\ 12 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ -1 \end{bmatrix}$$

---

3) Dokažite, da LWE problem, kjer je x izbran enakomerno naključno in e iz neke distribucije χ z majhnimi vrednostmi, ni težji od problema, kjer sta $\overline{x}$ in $\overline{e}$ izbrana iz iste distribucije χ.

Standardni LWE: $Ax + e = y$
Nestandardni LWE: $\overline{A}\overline{x} + \overline{e} = \overline{y}$

Potencialni problem: $\overline{x}$ je manj naključen

$$A = \begin{bmatrix} A_1 \\ A_2 \end{bmatrix}, \quad e = \begin{bmatrix} e_1 \\ e_2 \end{bmatrix}, \quad y = \begin{bmatrix} y_1 \\ y_2 \end{bmatrix}$$

$$\Rightarrow \begin{aligned} A_1 x + e_1 &= y_1 \quad \Rightarrow \quad x = A_1^{-1}(y_1 - e_1) \\ A_2 x + e_2 &= y_2 \end{aligned}$$

$$\Rightarrow A_2 A_1^{-1}(y_1 - e_1) + e_2 = y_2$$

$$\Rightarrow A_2 A_1^{-1} y_1 - A_2 A_1^{-1} e_1 + e_2 = y_2$$

$$\Rightarrow e_2 - A_2 A_1^{-1} e_1 = y_2 - A_2 A_1^{-1} y_1$$

Definiramo:

$$\begin{aligned} -A_2 A_1^{-1} &=: \overline{A} \\ e_1 &=: \overline{x} \\ e_2 &=: \overline{e} \\ y_2 - A_2 A_1^{-1} y_1 &=: \overline{y} \end{aligned}$$

Dobimo:

$$\overline{A}\overline{x} + \overline{e} = \overline{y}$$

---

4) Popravite LWE kriptosistem tako, da namesto $m \in \{0,1\}$ šifrira $m \in \mathbb{Z}_q$ za $q \ll p$.

$$\mathbb{Z}_q = \{0, 1, \ldots, q-1\}$$

Sporočila morajo biti dovolj narazen, da šum ne spremeni enega v drugega.

To lahko dosežemo tako, da sporočila pomnožimo s $\lfloor \frac{p}{2} \rfloor$ in dobimo nova enakomerno porazdeljena sporočila.

$\Rightarrow 0 \cdot \lfloor \frac{p}{2} \rfloor, 1 \cdot \lfloor \frac{p}{2} \rfloor, \dots, (q-1) \cdot \lfloor \frac{p}{2} \rfloor$

Šifriranje:

- Izberemo vektor $w \in \{0,1\}^{\text{št. vrstic } A}$
- $c_0 = w^T \cdot A$
- $c_1 = w^T \cdot y + H \cdot \lfloor \frac{p}{2} \rfloor$
- $c = (c_0, c_1)$

Desifriranje:

$$H' = c_1 - c_0 \cdot x = w^T \cdot \underbrace{y}_{Ax+e} + H \cdot \lfloor \frac{p}{2} \rfloor - w^T A \cdot x$$

$$= w^T \cdot Ax + w^T \cdot e + H \cdot \lfloor \frac{p}{2} \rfloor - w^T \cdot A \cdot x$$

$$= w^T \cdot e - H \cdot \lfloor \frac{p}{2} \rfloor$$

Konstruiramo H kot element v $\mathbb{Z}_q$, ki je najbližji $\frac{H'}{\lfloor \frac{p}{2} \rfloor}$.

Pogoj za pravilno desifriranje je $w^T e < \frac{1}{2} \lfloor \frac{p}{2} \rfloor$. Če to ne velja, bomo sporočili na naslednje bezedilo.

5) Kriptosistem iz naloge (4) uporabite za $q=5$, $p=53$, $m=2$,
$A=\begin{bmatrix}2&1\\0&3\\4&2\end{bmatrix}$, $e=\begin{bmatrix}2\\1\\3\end{bmatrix}$, $x=\begin{bmatrix}5\\1\end{bmatrix}$.

$$y = Ax+e = \begin{bmatrix}2&1\\0&3\\4&2\end{bmatrix}\begin{bmatrix}5\\1\end{bmatrix} + \begin{bmatrix}2\\1\\3\end{bmatrix} = \begin{bmatrix}13\\4\\25\end{bmatrix}$$

Izberemo $w=\begin{bmatrix}1\\0\\1\end{bmatrix}$.

$$c_0 = w^TA = \begin{bmatrix}1&0&1\end{bmatrix}\begin{bmatrix}2&1\\0&3\\4&2\end{bmatrix} = \begin{bmatrix}6&3\end{bmatrix}$$

$$c_1 = w^Ty + 2\cdot\left[\tfrac{53}{5}\right] = 38 + 2\cdot 10 = 58 = 5 \mod p$$

$$\Rightarrow c = (\begin{bmatrix}6&3\end{bmatrix}, 5)$$

$$H' = c_1 - c_0\cdot x = 5 - \begin{bmatrix}6&3\end{bmatrix}\begin{bmatrix}5\\1\end{bmatrix} = 5-33 = -28 = 25 \mod p$$

$\frac{H'}{\left[\frac{p}{q}\right]} = \frac{25}{10} = 2{,}5 \rightsquigarrow 3$ najbližji element v $\mathbb{Z}_q = \mathbb{Z}_3$

$w^Te = 5$, $\frac{1}{2}\left[\frac{p}{2}\right] = 5$

---

6) Naj bo p praštevilo in α, γ generatorja grupe $\mathbb{Z}_p^*$. Recimo, da znamo učinkovito računati diskretne logaritme za bazo α. Pokaži, da kako potem učinkovito računamo diskretne logaritme tudi za bazo γ.

Želimo izračunati $\gamma^x = \beta \mod p$, $x = \log_\gamma \beta$.

α generator $\Rightarrow \gamma = \alpha^{x_1} \bmod p,\ \beta = \alpha^{x_2} \bmod p$

$\Rightarrow (\alpha^{x_1})^x = \alpha^{x_2} \bmod p$

α generator

$\Rightarrow x_1 \cdot x = x_2 \bmod (p-1)$

$\Rightarrow x = x_2 x_1^{-1} \bmod (p-1)$

$= \log_\alpha \beta \cdot (\log_\alpha \gamma)^{-1} \bmod (p-1)$

19.4.

1) Naj bo p tako praštevilo, da je $p-1 = p_1 p_2 \cdots p_k$ produkt majhnih praštevil. Naj bo g generator grupe $\mathbb{Z}_p^*$ in $y \in \mathbb{Z}_p^*$ poljuben element. Opišite postopek, kako lahko hitro najdemo x, da velja $g^x \equiv y \bmod p$.

Za poljuben p_i naj bo $m_i = \frac{p-1}{p_i}$.

$(g^x)^{m_i} \equiv y^{m_i} \bmod p$

$(g^{m_i})^x \equiv y^{m_i} \bmod p$

Označimo: $h_i = g^{m_i}$, $z = y^{m_i}$

$h_i^x \equiv z \bmod p$

$\Rightarrow g$ generator reda $p-1$

$\Rightarrow h_i$ reda p_i

$\Rightarrow h_i$ generira podgrupo velikosti p_i

Dovolj je, da poiščemo $a_i \in \{0, 1, \ldots, p_i - 1\}$, da bo $h_i^{a_i} \equiv z_i \bmod p$.

$\Rightarrow x \equiv a_i \mod p_i$

Za vsak $i = 1, 2, \ldots, k$ imamo:

$x \equiv a_1 \mod p_1$
$x \equiv a_2 \mod p_2$
$\vdots$
$x \equiv a_k \mod p_k$

Po CRT dobimo $x \mod p-1$.