1) Alenka želi Borisu poslati zaupno sporočilo m in hkrati dokazati, da je sporočilo poslala ona. Alenka ima par ključev (n_A, e_A) in (n_A, d_A), Boris pa (n_B, e_B) in (n_B, d_B).

Alenka uporabi naslednji postopek:

1) Izračuna podpis $s = h(m)^{d_A} \bmod n_A$

2) Sporočilo m zašifrira kot $c = m^{e_B} \bmod n_B$ z Borisovim javnim ključem

3) Pošlje par (c, s) Borisu

a) Pojasnite, kako lahko Boris preveri pristnost podpisa.

b) Pokažite, kako lahko Boris zlorabi par (c, s) na način, da Cenetu pošlje ponarejen par (c', s) in ga prepriča, da je Alenka poslala sporočilo njemu. Cene ima ključa (n_C, e_C) in (n_C, d_C).

c) Kaj pa v primeru, da Alenka najprej šifrira sporočilo in šele nato pošlje? Kako v tem primeru Boris preveri pristnost sporočila? Ali lahko v tem primeru zlorabi par (c, s)?

a) 1. Dešifrira c: $m = c^{d_B} \bmod n_B$

2. Izračuna $h(m)$

3. Preveri $h(m) = s^{e_A} \bmod n_A$

$s^{e_A} = ((h(m))^{d_A})^{e_A} = h(m)^{n_A d_A} = h(m) \mod n_A$

b) 1. Izračuna $c' = m^{e_C} \mod n_C$

2. Pošlje (c', s)

c) Alenkin podpis je $s = h(s)^{d_A} \mod n_A$

Boris preveri podpis $h(c) = s^{e_A} \mod n_A$

Ne more dokazati, kaj je Alenka podpisala, brez da razbije d_B

---

2) Alenka ima javni ključ (n, e) in zasebni ključ (n, d) za RSA. Radi bi, da nam podpiše sporočilo m, ampak sporočila ne želimo razkriti. Zato podtaknemo v podpis sporočilo $m' = k \cdot m \mod n$. Privzamemo lahko, da je m tuj z n, sicer znamo razcepiti n in lahko podpišemo kamorkoli.

a) Kako moramo izbrati k, da bomo iz podpisa sporočila m', $s' = (m')^d \mod n$, lahko izračunali podpis sporočila m, ne da bi morali poznati zasebni ključ d?

b) Ilustrirajte na primeru $n = 85$, $e = 11$, $m = 42$.

a) $s' = (k \cdot m)^d = k^d \cdot m^d \mod n$

Izberemo $k = \ell^e \mod n$, $\gcd(\ell, n) = 1$

$k^d = \ell^{ed} = \ell \mod n$

$s' = \ell \cdot m^d \mod n$

$m^d = s' \cdot l^{-1} \bmod n = \underline{\underline{s}}$

b) $n = 85,\ e = 11,\ m = 42$

Izberemo $l := 2$

$\Rightarrow \gcd(2, 85) = 1$ ✓

$k = 2^{11} = 2048 = 8 \bmod 85$

$\Rightarrow m' = k \cdot m = 8 \cdot 42 = 336 = 81 \bmod 85$

$n = 85 = 17 \cdot 5 \Rightarrow \varphi(n) = 16 \cdot 4 = 64$

$11d = 1 \bmod 64 \Rightarrow d = 35$

$\Rightarrow s' = 81^{35} \bmod 85 = 21 \bmod 85$

$s = 42^d = 21 \cdot 2^{-1} \bmod 85 = 21 \cdot 43 = 53 \bmod 85$

---

3) Alenka je objavila vrednosti za Elgamalov podpis $p = 173$, $\alpha = 2$, $\beta = 83$. Izbere $k = 9$ in izračuna $r = \alpha^k = 166 \bmod 173$. Pošlje Borisu sporočili $(16, 166, 160)$ in $(40, 166, 48)$, pri čemer je za oba podpisa uporabila isti k.

Razložite, kako lahko Eva, ki prestreže obe sporočili, izračuna zasebni ključ od Alenke a in ponaredi njen podpis.

Velja: $\beta = \alpha^a \bmod p$, $r = \alpha^k \bmod p$

s izračunamo iz enačbe $m = a \cdot r + k \cdot s \bmod p-1$

$(m_1, r_1, s_1) = (16, 166, 160)$

$(m_2, r_2, s_2) = (40, 166, 48)$

$r_1 = r_2 = 166 = r$

$a \cdot r = m_1 - k \cdot s_1 \mod p-1$
$a \cdot r = m_2 - k \cdot s_2 \mod p-1$

$\Rightarrow m_1 - k \cdot s_1 = m_2 - k \cdot s_2 \mod p-1$

$\Rightarrow m_1 - m_2 = (s_1 - s_2)k \mod p-1$

$\Rightarrow -24 = 112 \cdot k \mod 172$

$\Rightarrow 112k = 148 \mod 172$

$\gcd(112, 172) = 4$

$4 \mid 148 \Rightarrow 28k = 37 \mod 43$

$\Rightarrow 28^{-1} = 20 \mod 43$

$\Rightarrow k = 20 \cdot 37 = 9 \mod 43$

$\Rightarrow k \in \{9 + 0 \cdot 43, 9 + 1 \cdot 43, 9 + 2 \cdot 43, 9 + 3 \cdot 43\}$

$r = \alpha^k \mod p$

$\Rightarrow 2^k = 166 \mod 172$

Preverimo in dobimo $k = 9$

$a \cdot r = m - k \cdot s \mod p$

$166a = 16 - 9 \cdot 160 \mod 172$

$\gcd(166, 172) = 2$

$\Rightarrow 83a = 62 \mod 86$

$\vdots$

$\Rightarrow a = 8$

---

4) Alenka ima spet vrednosti za Elgamalov podpis $p = 173$, $\alpha = 2$, $\beta = 83$. Pošlje sporočili Borisu $(25, 26, 101)$ in $(35, 26, 167)$. Ponovno pokažite, kako ponarediti njen podpis.

DN

---

5) Alenka uporabi DSA (digital signature algorithm) za podpisovanje. Naj bo $g = 43$ in $p = 173$, $q = 2$ in $\alpha = g^{\frac{p-1}{q}} = 16 \mod 173$. Naj bo $a = 7$, $\beta = \alpha^a = 6 \mod 173$. Alenka objavi $(173, 43, 16, 6)$. Predpostavimo, da je zgoščena vrednost sporočila, ki ga želimo poslati, $h(m) = 30$ in $k = 9$. Izračunajte par (r, s) in preverite pristnost podpisa.

DN

---

6) Definiran je protokol:

$A \rightarrow B: E_{k_B}(k)$

$B \to A: E_k(n_B)$

$A \to B: E_k(S_{k_{dA}}(n_B))$

a) Razložite, kaj protokol poskuša doseči.

b) Preverite varnost protokola.

a) Namen je izmenjava in overitev ključa k.

b) C napadalec

$C \to B: E_{k_B}(k)$

C dobi n_B

$C \to B: E_k(S_{k_{dA}}(n_B))$

$\Rightarrow$ B misli, da govori z A

$A \to C: E_{k_C}(k')$

$C \to A: E_{k'}(n_B)$

$A \to C: E_{k'}(S_{k_{dA}}(n_B))$

$\Rightarrow$ Ni varno