Cryptography

Homework 5

$\alpha = 10$, $p = 971$, $q = 97$, $s = 314$, generator $r = 8$

1a) $h = s^x \bmod p$ where $x = 23$

$h = 314^{23} \bmod 971$

Used calculator → $h = 865$ $(h, p) \rightarrow (865, 971)$

b) Encryption: $m = 49$

1. Ephemeral key: $k = 29$

Used calculator:

2. $C_1 = s^k = 314^{29} \bmod 971 = 364$

3. $C_2 = m \cdot h^k = 49 \cdot 865^{29} \bmod 971$
$= 448$

4. Ciphertext $C = (C_1, C_2) = (364, 448)$

c) Decryption: $C = (364, 448)$ and $x = 23$

$m = \frac{C_2}{C_1^x} \bmod p = \frac{448}{364^{23}} \bmod 971$

$= 448 \cdot 364^{-23} \bmod 971$

$364^{-23} \Rightarrow 364 = 314^{29}$

$364^{-1} = 314^{68}$ ← because $97 + 29$

$314^{97} = 1 \bmod p$

$364 \cdot 364^{-1} = 1 \bmod p$

$314^{29} \cdot 314^{68} = 1 \bmod 971$

$1564 = 97 \cdot 5 + 12$

$\rightarrow (364^{-1})^{23} = (314^{68})^{23} \bmod 971$

$= 314^{1564} \bmod 971$

$= (314^{97})^5 \bmod 971$

$= 314^{12} \bmod 971$

Find $448 \cdot 314^{12} \bmod 971$

Used calculator: (49) ✓

d) Encryption: $m = 49$

1. Ephemeral key: $k = 135$

2. $C_1 = s^k = 314^{135} \bmod 971 = 730$

3. $C_2 = m \cdot h^k = 49 \cdot 865^{135} \bmod 971$
$= 821$

4. Ciphertext $C = (C_1, C_2) = (730, 821)$

e) Decryption: $C = (730, 821)$ and $x = 23$

$$m = \frac{c_2}{c_1^x} \bmod p = \frac{821}{730^{23}} \bmod 971$$

$$= 821 \cdot 730^{-23} \bmod 971$$

can be rewritten as

$$(730^{-1})^{23} \bmod 971$$

$730^{-1} \bmod 971 = 278$

Extended Euclidean Algorithm

$971 = 730 \cdot 1 + 241$ $\quad 241 = 971 - 730 \cdot 1$

$730 = 241 \cdot 3 + 7$ $\quad 7 = 730 - 241 \cdot 3$

$241 = 7 \cdot 34 + 3$ $\quad 3 = 241 - 7 \cdot 34$

$7 = 3 \cdot 2 + 1 \rightarrow 1 = 7 - 3 \cdot 2$

Substitution

$1 = 7 - (241 - 7 \cdot 34) \cdot 2$

$= 7 \cdot 69 - 241 \cdot 2$

$= (730 - 241 \cdot 3) \cdot 69 - 241 \cdot 2$

$= 730 \cdot 69 - 241 \cdot 209$

$= 730 \cdot 69 - (971 - 730 \cdot 1) \cdot 209$

$= 730 \cdot 278 - 971 \cdot 209$

(278)

$(278)^{23} \bmod 971$ use calculator

$= 770$

$821 \cdot 770 \bmod 971$ use calculator

$= 49$ ✓

f) The ciphertexts are different because you are using a different k ephemeral key to calculate c_1 and c_2. They give the same message because all the other parameters such as the private key and message. All you are doing is using a different encryption key to encrypt the same message. So, you will definitely obtain the same message.

2) $m = 71$, $\mathbb{Z}^*_{971}$, generator $\alpha = 8$, $k_{priv} = 23 = a$

a) public key $k_{pub} = (p, \alpha, \beta)$ used calculator

$\beta = \alpha^a \bmod p = 8^{23} \bmod 971 = 804$

$k_{pub} = (971, 8, 804)$

b) Signing

1. $k = 53$ $\quad \gcd(53, 970) = 1$
2. $\text{Sign}(x, k) = (\gamma, \delta)$

$\gamma = \alpha^k \bmod p = 8^{53} \bmod 971 = 813$

$\delta = (m - a\gamma)k^{-1} \bmod p-1 = (71 - 23 \cdot 813)53^{-1} \bmod 970$

Extended Euclid Algorithm ←

$970 = \underline{53} \cdot 18 + \underline{16} \rightarrow 16 = 970 - 53 \cdot 18$

$53 = \underline{16} \cdot 3 + \underline{5} \rightarrow 5 = 53 - 16 \cdot 3$

$16 = \underline{5} \cdot 3 + \underline{1} \rightarrow 1 = 16 - 5 \cdot 3$

$5 = \underline{1} \cdot 5 + \underline{0}$

Substitution:

$1 = 16 - (53 - 16 \cdot 3) \cdot 3$

$= 16 \cdot 10 - 53 \cdot 3$

$= (970 - 53 \cdot 18) \cdot 10 - 53 \cdot 3$

$= 970 \cdot 10 - 53 \cdot 183$

$= 970 - 183 = 787 \bmod 970$

$\rightarrow 787 \cdot (71 - 23 \cdot 813) \bmod 970 = 344 = \delta$

$\text{Sign}_{k_{priv}}(813, 344)$

c) Verify

$\text{Verify}_{k_{pub}}(m, (\gamma, \delta)) \rightarrow \beta^\gamma \cdot \gamma^\delta \bmod p$

$= 804^{813} \cdot 813^{344} \bmod 971 = 371 \cdot 628 \bmod 971$

$= 919$

$919 = \alpha^m \bmod p$

$= 8^{71} \bmod 971$ <= Used calculator

$919 \equiv 919$ Verified!

3. $p = 43, q = 37, b = 23$

a) $N = p \cdot q = 1591$ $\quad \phi(N) = (p-1)(q-1)$

$= (43-1)(37-1) = 1512$

$k_{priv} = a = b^{-1} \bmod \phi(N)$

$= 23^{-1} \bmod 1512$

Extended Euclidean Algorithm

$1512 = \underline{23} \cdot 65 + \underline{17}$ $\quad 6 = \underline{5} \cdot 1 + \underline{1}$

$23 = \underline{17} \cdot 1 + \underline{6}$ $\quad 5 = \underline{1} \cdot \underline{5} + \underline{0}$

$17 = \underline{6} \cdot 2 + \underline{5}$ $\quad \gcd(1512, 23) = 1$

$17 = 1512 - 23 \cdot 65$

$6 = 23 - 17 \cdot 1$

$5 = 17 - 6 \cdot 2$

$1 = 6 - 5 \cdot 1$

Substitution

$1 = 6 - (17 - 6 \cdot 2) \cdot 1$

$= 6 \cdot 3 - 17 \cdot 1$

$= (23 - 17 \cdot 1) \cdot 3 - 17 \cdot 1$

$= 23 \cdot 3 - 17 \cdot 4$

$= 23 \cdot 3 - (1512 - 23 \cdot 65) \cdot 4$

$= 23 \cdot 263 - 4 \cdot 1512$

$263 = a = k_{priv}$

b) Signing $X = 91$

$Sign_{priv}(X) = X^a \bmod N = 91^{263} \bmod 1591$

used calculator $\rightarrow \doteq 550 = y$

(Sign, message) = (550, 91)

c) Verification

$y^b \bmod N \stackrel{?}{\doteq} X$

used calculator $\rightarrow 550^{23} \bmod 1591 \stackrel{?}{\doteq} 91$

$91 \stackrel{\checkmark}{=} 91$ Verified!