CS 4801: Assignment 5

Adam Camilli (aocamilli@wpi.edu)

Wednesday 12th December, 2018

1. **ElGamal Encryption:** Encrypt and decrypt the following messages using ElGamal Encryption for $\mathbb{Z}_{971}^*$ and $g = 314$ (generator $r = 8$ and $\alpha = 10$, $q = 97$) and show every intermediate step:

   (a) Find the public key for private key $x = 23$.

   $$\beta = g^x \bmod p = 314^{23} \bmod 971 = 865$$

   $$k_{pub} = \big(p, g, \beta\big) = \big(971, 314, 865\big)$$

   (b) Encrypt the message $m = 49$ with random parameter $k = 29$.

   $$e_{k_{pub}}(x, k) = \big(Y_1, Y_2\big)$$

   $$Y_1 = g^k \bmod p = 314^{29} \bmod 971 = 364$$
   $$Y_2 = m \cdot \beta^k \bmod p = 49 \cdot 865^{29} \bmod 971 = 448$$

   $$\big(Y_1, Y_2\big) = (\mathbf{364, 448})$$

   (c) Decrypt the ciphertext from part b.

   $$\begin{aligned} m &= d_{k_{priv}}\big(Y_1, Y_2\big) \\ &= Y_2\big(Y_1^x\big)^{-1} \bmod p \\ &= 448 \cdot 364^{-23} \bmod 971 \\ &= 448 \cdot (364^{-1})^{23} \bmod 971 \end{aligned}$$

   (next page)

$$
\begin{array}{ll}
s_0: \ 971 = \mathbf{2}(364) + 243 & p_0 = 0 \text{ (given)} \\
s_1: \ 364 = \mathbf{1}(243) + 121 & p_1 = 1 \text{ (given)} \\
s_2: \ 243 = \mathbf{2}(121) + 1 & p_2 = p_0 - p_1(q_0) \bmod 971 \\
 & \quad = 0 - 1(2) \bmod 971 = 969 \\
s_3: \ 121 = \mathbf{121}(1) + 0 & p_3 = p_1 - p_2(q_1) \bmod 971 \\
 & \quad = 1 - 969(1) \bmod 971 = 3 \\
 & p_4 = p_2 - p_3(q_2) \bmod 971 \\
 & \quad = 969 - 3(2) \bmod 971 = \mathbf{963}
\end{array}
$$

$$m = 448 \cdot (963)^{23} \bmod 971 = 49$$

(d) Encrypt the message $m = 49$ with random parameter $k = 135$

$$e_{k_{pub}}(x, k) = \big(Y_1, Y_2\big)$$

$$
\begin{aligned}
Y_1 &= g^k \bmod p = 314^{135} \bmod 971 = 730 \\
Y_2 &= m \cdot \beta^k \bmod p = 49 \cdot 865^{135} \bmod 971 = 821
\end{aligned}
$$

$$\big(Y_1, Y_2\big) = (\mathbf{720, 821})$$

(e) Decrypt the ciphertext from part d.

$$
\begin{aligned}
m &= d_{k_{priv}}\big(Y_1, Y_2\big) \\
&= Y_2\big(Y_1^x\big)^{-1} \bmod p \\
&= 821 \cdot 730^{-23} \bmod 971 \\
&= 821 \cdot (730^{-1})^{23} \bmod 971
\end{aligned}
$$

$$
\begin{array}{ll}
s_0: \ 971 = \mathbf{1}(730) + 241 & p_0 = 0 \text{ (given)} \\
s_1: \ 730 = \mathbf{3}(241) + 7 & p_1 = 1 \text{ (given)} \\
s_2: \ 241 = \mathbf{34}(7) + 3 & p_2 = p_0 - p_1(q_0) \bmod 971 \\
 & \quad = 0 - 1(1) \bmod 971 = 970
\end{array}
$$

(next page)

$s_3: \ 7 = \mathbf{2}(3) + 1$

$s_4: \ 3 = \mathbf{3}(1) + 0$

$$\begin{aligned} p_3 &= p_1 - p_2(q_1) \bmod 971 \\ &= 1 - 970(3) \bmod 971 = 4 \\ p_4 &= p_2 - p_3(q_2) \bmod 971 \\ &= 970 - 4(34) \bmod 971 = 834 \\ p_5 &= p_3 - p_4(q_3) \bmod 971 \\ &= 4 - 834(2) \bmod 971 = \mathbf{278} \end{aligned}$$

$$m = 821 \cdot (278)^{23} \bmod 971 = 49$$

(f) In part b. and d, the same message is encrypted under the same private key with different ephemeral keys. Explain why the related ciphertexts are different and how they give the same message m after decryption.

A shortcoming of the base algorithm is that if an attacker finds the ephemeral key k, they can recover m:

$$m = Y_1 \cdot \beta^{-k} \bmod p$$

k must therefore be random each time (and realistically p must be on the order of 1024 bits).

The ciphertexts are of course different since they are calculated with different k, but they give the same message m after decryption since the secret key is the same for both (and is the only thing other ciphertexts used for decryption). This works because the public key was generated from the secret key and is only manipulated by k as an exponent in the ciphertext calculations:

$$\begin{aligned} Y_1 &= g^k \bmod p \\ Y_2 &= m \cdot \beta^k \bmod p \end{aligned}$$

which means the decryptions are mathemcatically equivalent mod p regardless of the value of k.

2. **ElGamal Signature:** Sign and verify the message $m = 71$ using Elgamal Signature Scheme for $\mathbb{Z}_{971}^*$, generator $\alpha = 8$ and private key $x = 23$. Show every intermediate step:

   (a) Find the public key.

$$\begin{aligned}\beta &= \alpha^x \bmod p = 8^{23} \bmod 971 \\ &= 804\end{aligned}$$

$$k_{pub} = \big(p, \alpha, \beta\big) = \big(971, 8, 804\big)$$

   (b) Sign the given message ($m = 71$) using the ephemeral key $k = 53$.

$$sig_{k_{priv}} = (\gamma, \delta)$$

$$\begin{aligned}\gamma &= \alpha^k \bmod p = 8^{53} \bmod 971 = \mathbf{813} \\ \delta &= (m - k_{priv} \cdot \gamma) \cdot k^{-1} \bmod p - 1 \\ &= (71 - 23 \cdot 813) \cdot 53^{-1}) \bmod 970 \\ &\dots\end{aligned}$$

$$\begin{aligned}
s_0 &: \ 970 = \mathbf{18}(53) + 16 & p_0 &= 0 \text{ (given)} \\
s_1 &: \ 53 = \mathbf{3}(16) + 5 & p_1 &= 1 \text{ (given)} \\
s_2 &: \ 16 = \mathbf{3}(5) + 1 & p_2 &= p_0 - p_1(q_0) \bmod 970 \\
& & &= 0 - 1(18) \bmod 970 = 952 \\
s_3 &: \ 5 = \mathbf{5}(1) + 0 & p_3 &= p_1 - p_2(q_2) \bmod 970 \\
& & &= 1 - 952(3) \bmod 970 = 55 \\
& & p_4 &= p_2 - p_3(q_3) \bmod 970 \\
& & &= 952 - 55(3) \bmod 970 = \mathbf{787}
\end{aligned}$$

$$\begin{aligned}&\dots \\ \delta &= (71 - 23 \cdot 813) \cdot 787 \bmod 970 \\ &= \mathbf{344}\end{aligned}$$

(c) Verify the signature computed in part b.

$$\begin{aligned} ver_{k_{pub}} &= \beta^{\gamma} \cdot \gamma^{\delta} \equiv \alpha^{m} \bmod p \text{ if valid} \\ &= 804^{813} \cdot 813^{344} \bmod 971 \equiv 8^{71} \bmod 971 = \mathbf{919} \end{aligned}$$

3. **RSA Signature** Let $p = 43$, $q = 37$, public key $b = 23$ be your initial parameters. You may use a calculator for this problem, but you should show all intermediate results.

   (a) Key generation: Compute N and $\phi(N)$. Compute the private key $k_{priv} = a = b^{-1} \bmod \phi(N)$. Show all intermediate results.

$$N = pq = 43 \cdot 37 = 1591$$
$$\phi(N) = (p-1)(q-1) = 42 \cdot 36 = 1512$$
$$a = b^{-1} \bmod \phi(N) = 23^{-1} \bmod 1512$$

$s_0: \ 1512 = \mathbf{65}(23) + 17$	$p_0 = 0$ (given)
$s_1: \ 23 = \mathbf{1}(17) + 6$	$p_1 = 1$ (given)
$s_2: \ 17 = \mathbf{2}(6) + 5$	$p_2 = p_0 - p_1(q_0) \bmod 1512$
	$= 0 - 1(65) \bmod 1512 = 1447$
$s_3: \ 6 = \mathbf{1}(5) + 1$	$p_3 = p_1 - p_2(q_1) \bmod 1512$
	$= 1 - 1447(1) \bmod 1512 = 66$
$s_4: \ 5 = \mathbf{1}(5) + 0$	$p_4 = p_2 - p_3(q_2) \bmod 1512$
	$= 1447 - 66(2) \bmod 1512 = 1315$
	$p_5 = p_3 - p_4(q_3) \bmod 1512$
	$= 66 - 1315(1) \bmod 1512 = \mathbf{263}$

$$k_{\text{priv}} = \mathbf{263}$$

   (b) Signing: Sign the message $X = 91$.

$$sig_{k_{priv}}(x) = x^a \bmod n$$
$$= 91^{263} \bmod 1591$$
$$= \mathbf{550}$$

   (c) Verification: Verify the signature $Sign(X)$ computed in part b.

$$ver_{k_{pub}}(x, y) = y^b \bmod N = x \text{ if valid}$$
$$= 550^{23} \bmod 1591 = \mathbf{91}$$