[CSCI 55500] Homework 3
David Xu

All attached code was written in Python3 (3.6.1).

1. $24^{66,000,000,023} \bmod 77$

$$
\begin{aligned}
24^{10} \bmod 11 &= 1 \\
24^{10(6,600,000,002)+3} &= 24^3 \bmod 11 \\
&= (2^3)^3 \bmod 11 \times 3^3 \bmod 11 \\
&= 6 \times 5 \bmod 11 \\
a_1 &\equiv 8
\end{aligned}
$$

$$
\begin{aligned}
24^6 \bmod 7 &= 1 \\
24^{6(11,000,000,003)+5} &= 24^5 \bmod 7 \\
&= (2^3)^5 \bmod 7 \times 3^5 \bmod 7 \\
&= 1 \times 5 \bmod 7 \\
a_2 &\equiv 5
\end{aligned}
$$

$$
\begin{aligned}
M_1 &= \frac{M}{m_1} = \frac{77}{11} = 7 \\
y_1 &= 7^{-1} \bmod 11 \equiv 8 \\
M_2 &= \frac{M}{m_2} = \frac{77}{7} = 11 \\
y_2 &= 11^{-1} \bmod 7 \equiv 2
\end{aligned}
$$

$$
\begin{aligned}
\sum_i (a_i M_i y_i) \bmod M &= (8 \times 7 \times 8) + (5 \times 11 \times 2) \pmod{77} \\
&= 558 \bmod 77 \\
&\equiv 19
\end{aligned}
$$

2. ElGamal Plaintext:
shestandsupinthegardenwhereshehasbeenworkingandlooksintothedistanceshehassensedachangeintheweatherther
eisanothergustofwindabuckleofnoiseintheairandthetallcypressesswaysheturnsandmovesuphilltowardsthehouse
climbingoveralowwallfeelingthefirstdropsofrainonherbarearmsshecrossestheloggiaandquicklyentersthehouse

For each (y_1, y_2), I decrypted using,

$$
\begin{aligned}
d_K(y_1, y_2) &= y_2 (y_1^a)^{-1} \bmod p \\
&= y_2((y_1^a)^{-1} \bmod p) \bmod p
\end{aligned}
$$

For example, if $(y_1, y_2) = (3781, 14409)$,

$$
\begin{aligned}
d_K(3781, 14409) &= 14409((3781^{7899})^{-1} \bmod 31847) \bmod 31847 \\
&= 14409(6479) \bmod 31847 \\
&= 12354
\end{aligned}
$$

Then I solved for

$$
\begin{aligned}
X &= 26^2 x_1 + 26^1 x_2 + x_3 \\
x_3 &= X \bmod 26 \\
x_2 &= \frac{X - x_3}{26} \bmod 26
\end{aligned}
$$

$$x_1 = \frac{X - x_3 - x_2}{26^2} \bmod 26$$

$$(x_1, x_2, x_3) = (18,7,4) = (s, h, e)$$

3. RSA Common Modulus protocol
   a.

$$\begin{aligned}
y_1 &= x^{b_1} \bmod n \\
y_2 &= x^{b_2} \bmod n \\
c_1 &= b_1^{-1} \bmod b_2 \\
c_2 &= \frac{c_1 b_1 - 1}{b_2} \\
x_1 &= y_1^{c_1}\left(y_2^{c_2}\right)^{-1} \bmod n \\
&= x^{b_1 c_1}\left(x^{b_2 c_2}\right)^{-1} \bmod n \\
&= x^{b_1 b_1^{-1} \bmod b_2}\left(x^{b_2\left(\frac{c_1 b_1 - 1}{b_2}\right)}\right)^{-1} \bmod n \\
&= x^{b_1 b_1^{-1} \bmod b_2}\left(x^{b_1 b_1^{-1} \bmod b_2 - 1}\right)^{-1} \bmod n \\
&= x^{b_1 b_1^{-1} \bmod b_2} - x^{b_1 b_1^{-1} \bmod b_2 + 1} \bmod n \\
&= x \bmod n
\end{aligned}$$

   b.

$$\begin{aligned}
c_1 &= b_1^{-1} \bmod b_2 = 2692 \\
c_2 &= \frac{c_1 b_1 - 1}{b_2} = 15 \\
x_1 &= y_1^{c_1}\left(y_2^{c_2}\right)^{-1} \bmod n = 15001
\end{aligned}$$

4. Elliptic curve $E = y^2 = x^3 + x + 6, Z_{1039}$
   a. For $x = 0 \ldots 1038$, first compute z. For example, for $x = 10$,

$$\begin{aligned}
z &= x^3 + x + 6 \bmod 1039 \\
&= 10^3 + 10 + 6 \bmod 1039 \\
&= 1016
\end{aligned}$$

   Then check if z is a quadratic residue,

$$\begin{aligned}
\left(\frac{z}{p}\right) &= \left(\frac{1016}{1039}\right) \\
&= z^{\frac{p-1}{2}} \bmod p \\
&= 1016^{\frac{1039-1}{2}} \bmod 1039 \\
&= 1
\end{aligned}$$

   If $\left(\frac{z}{p}\right) = 1$, then z is a quadratic residue of p, and the point is found by,

$$\begin{aligned}
y &= \pm z^{\frac{p+1}{4}} \bmod p \\
&= \pm 1016^{\frac{1039+1}{4}} \bmod 1039 \\
&= \pm 492 \bmod 1039 \\
&= 492, 547
\end{aligned}$$

Giving the 2 points $(10, 492)$ and $(10, 547)$. In total, there are 1008 points on E.

b. The maximum point is $(1038, 1037)$.

c. $(1014, 291)$ is not in E. The 2 points when $x = 1014$ are $(1014, 290)$ and $(1014, 749)$.

d. Ciphertext:

$$y_1 = k\alpha = 100 \times (799{,}790) = (873, 233)$$
$$y_2 = x + k\beta = (575{,}419) + (986{,}213) = (963{,}817)$$

Plaintext:

$$x = y_2 - ky_1 = (234{,}14) - 100 \times (873{,}233) = (234{,}14) - (498{,}502)$$
$$= (234{,}14) + (498{,}537) = (811{,}122)$$

e. Diffie-Hellman key exchange

Brute force Alice's key:

$$A = a\alpha$$
$$a = (199, 72)$$

Then compute the shared secret:

$$K = aB = (191{,}568)$$

5. Security
   1. None

      C: not guaranteed by XOR of hash of s_k with m

      I: not guaranteed by any hash of the message, only from hash of s_k

      A: since there is no signature, only way to authenticate is to $E_{S_{pub}}\left(D_{R_{pri}}\left(E_{R_{pub}}(s_k)\right)\right) =$

      $E_{S_{pub}}(S_k)$ of a random session key.

      NR: No signature, only knowledge that m is from S is that hash of s_k is XOR with message with a random session key
   2. C, I, A

      C: Guaranteed by encrypted message and hash of k_2 with message

      I: Guaranteed by hash

      A: guaranteed by mutual keys

      NR: No signature
   3. C, I, A, R

      C: Encrypted by public key of receiver

      I: Verifiable by $H(x)$

      A: Verifiable if signature of $H(x)$ is equivalent to the message

      NR: Verifiable if signature of $H(x)$ is equivalent to the message
   4. C, A, NR

      C: Via encryption by symmetric key

      I: No hash of message

      A: Via comparison $E_{S_{pub}}\left(D_{R_{pri}}\left(E_{R_{pub}}(s_k)\right)\right) = E_{S_{pub}}(S_k)$

      NR: Via signature of symmetric key

6. ElGamal Signature

$$sig(m) = (\gamma, \delta)$$
$$\gamma = \alpha^k$$
$$\delta = k^{-1}(m - a\gamma) \bmod (p - 1)$$
$$\delta k = (m - a\gamma) \mathrm{mod}\ (p - 1)$$
$$\delta k + a\gamma = m \bmod (p - 1)$$
$$a\gamma = m \bmod (p - 1)$$
$$a = my^{-1} \bmod (p - 1)$$
$$a = m\left(\alpha^k\right)^{-1} \bmod (p - 1)$$

Where p is part of the public key, m is the signed message, and γ is part of the signature. Have both a message and the corresponding signature means that a is easily computable as this is no longer an example of a discrete logarithm problem.