Exercise Sheet 5

Josh Wainwright
UID:1079596

1 Diffie-Hellman Key Exchange

$$p = 23,\ g = 3,\ a = 17,\ b = 11 \tag{1}$$

1. Alice and Bob agree (publicly) on a prime number, $p = 23$ (ie on $\mathbb{Z}_p^*$) and on an element $g \in \mathbb{Z}_p^*$ that generates the finite group G_q.
2. Alice picks a random positive integer $a = 17$ and sends $g^a = 3^{17} = 129140163$ to Bob.
3. Bob picks a random positive integer $b = 11$ and sends $g^a = 3^{11} = 177147$ to Alice.
4. Alice computes the key $K = \left(g^b\right)^a = (177147)^{17}$.
5. Bob computes the key $K = \left(g^b\right)^a = (129140163)^{11}$.
6. Both Alice and Bob now have the same key, $K = 166599860176309800046026634524986233548179040667038295235391424284221259369213254148867387$

2 ElGammel

$$p = 47,\ q = 23,\ g = 2,\ \Rightarrow G_{23} = \langle 2 \rangle \tag{2}$$
$$x = 6,\ y = 10,\ M = 9 \tag{3}$$

2.1 Key Generation

1. Generate primes $p = 47$ and $q = 23$ as well as an element $g \in \mathbb{Z}_p^*$ that generates the subgroup $G_q = G_{23} = \langle 2 \rangle$.
2. Choose a random $x = 6$ from $\{0, \dots, 22\}$.
3. Compute $h = g^x \mod p = 2^6 \mod 47 = 17$.
4. Publish the public key $\hat{K} = (G_q, q, g, h) = (\{1, 2, 4, 8, 16, 9, 18, 13, 3, 6, 12\}, 23, 23, 2, 17)$.
5. Retain the private key $K = x$.

2.2 Encryption

1. The message, M, is considered to be an element of G.
2. Choose a random $y = 10$ from $\{0, \dots, 22\}$ then calculate $c_1 = g^y = 1024$ and $c_2 = M \cdot h^y = 10376293541461622784$.
3. The ciphertext is then $C = (c_1, c_2) = (1024, 10376293541461622784)$.

2.3 Decryption

1. Using the secret key $K = x = 6$,
2. Compute

$$\begin{aligned} M &= c_2 \cdot {c_1}^{-x} \\ &= c_2 \cdot \left({c_1}^{-1}\right)^x \\ &= 10376293541461622784 \times \left(1024^{-1}\right)^6 \\ &= 9 \end{aligned}$$

3 RSA Encryption

$$p = 7,\ q = 11,\ e = 17,\ M = 48 \tag{4}$$

3.1 Key Generation

1. Generate two random primes $p = 7$ and $q = 17$.
2. Compute $n = pq = 7 \times 17 = 119$ and $\phi = (p-1)(q-1) = 6 \times 16 = 96$.
3. Select a random integer $e = 17$, $1 < e < \phi$ such that $\gcd(e, \phi) = 1$.
4. Use the extended Euclidean algorithm to compute the unique integer $d = 17$, $1 < d < \phi$, such that $\text{e} \times \text{d} \equiv 1 \mod (\phi)$.
5. Alice's public key is $(n, e) = (119, 17)$, and Alice's private key is $d = 17$

3.2 Encryption

1. Bob obtains Alice's public key $(n, e) = (119, 17)$.
2. Bobs computes the ciphertext, c,

$$\begin{aligned} c &= M^e \mod n \\ &= 48^{17} \mod 119 = 48. \end{aligned}$$

   and send c to Alice.

3.3 Decryption

1. Alice receives the ciphertext, c, from Bob and recovers the plaintext, $M = c^d \mod n$, with the private key, d,

$$\begin{aligned} M &= c^d \mod n \\ &= 48^{17} \mod 119 = 48. \end{aligned}$$

4 Invertible Elements of $\mathbb{Z}_{34}$

The members of $(\mathbb{Z}_{34}^{*}, \cdot)$ is not a group, but we can find the members of this set that have multiplicative inverses, elements x for which an element y exists such that $xy \equiv 1 \mod 34$.

We can disregard all the even elements since these all share a divisor with 34, namely 2, as well as the element 17. We know that there must be 16 invertable elements. The remaining elements of the multiplication table modulo 34 is shown below.

	1	**3**	**5**	**7**	**9**	**11**	**13**	**15**	**17**	**19**	**21**	**23**	**25**	**27**	**29**	**31**	**33**
1	***1***	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	33
3		9	15	21	27	33	5	11	17	23	29	***1***	7	13	19	25	31
5			25	***1***	11	21	31	7	17	27	3	13	23	33	9	19	29
7				15	29	9	23	3	17	31	11	25	5	19	33	13	27
9					13	31	15	33	17	***1***	19	3	21	5	23	7	25
11						19	7	29	17	5	27	15	3	25	13	***1***	23
13							33	25	17	9	***1***	27	19	11	3	29	21
15								21	17	13	9	5	***1***	31	27	23	19
17									17	17	17	17	17	17	17	17	17
19										21	25	29	33	3	7	11	15
21											33	7	15	23	31	5	13
23												19	31	9	21	33	11
25													13	29	11	27	9
27														15	***1***	21	7
29															25	15	5
31																9	3
33																	***1***

Thus, the invertible elements of $(\mathbb{Z}_{34}^{*}, \cdot)$ are 1, 3, 5, 7, 9, 11, 13, 15, 19, 21, 23, 25, 27, 29, 31, and 33.

Member of $(\mathbb{Z}_{34}^{*}, \cdot)$	Inverse, x^{-1}
3	23
5	7
9	19
11	31
13	21
15	25
27	29
33	33

5 Extended Euclidean Algorithm

$$a = 78, \, b = 127 \tag{5}$$

$$\begin{array}{rrl}
 & \gcd(a,b) = a * x + b * y & \\
(1) & 78 = 1 * 78 + 0 * 127 & \\
(2) & 127 = 0 * 78 + 1 * 127 & \\
 & & 127 > 78 \Rightarrow 127 \operatorname{div} 78 = 1 \\
(1) & 78 = 1 * 78 + 0 * 127 & \\
(2) := (2) - (1) & 49 = -1 * 78 + 1 * 127 & \\
 & & 78 > 49 \Rightarrow 78 \operatorname{div} 49 = 1 \\
(1) := (1) - (2) & 29 = 2 * 78 - 1 * 127 & \\
(2) & 49 = -1 * 78 + 1 * 127 &
\end{array}$$

$$49 > 29 \Rightarrow 49 \operatorname{div} 29 = 1$$

$$\begin{aligned} (1) \qquad & 29 = 2*78 - 1*127 \\ (2) := (2) - (1) \qquad & 20 = -3*78 + 2*127 \end{aligned}$$

$$29 > 20 \Rightarrow 29 \operatorname{div} 20 = 1$$

$$\begin{aligned} (1) := (1) - (2) \qquad & 9 = 5*78 - 3*127 \\ (2) \qquad & 20 = -3*78 + 2*127 \end{aligned}$$

$$20 > 9 \Rightarrow 20 \operatorname{div} 9 = 2$$

$$\begin{aligned} (1) \qquad & 9 = 5*78 - 3*127 \\ (2) := (2) - 2*(1) \qquad & 2 = -13*78 + 8*127 \end{aligned}$$

$$9 > 2 \Rightarrow 9 \operatorname{div} 2 = 8$$

$$\begin{aligned} (1) := (1) - 8*(2) \qquad & 1 = 57*78 - 35*127 \\ (2) \qquad & 2 = -13*78 + 8*127 \end{aligned}$$

$$2 > 1 \Rightarrow 2 \operatorname{div} 1 = 2$$

$$\begin{aligned} (1) \qquad & 1 = 57*78 - 35*127 \\ (2) := (2) - 2*(1) \qquad & 0 = -127*78 + 78*127 \end{aligned}$$

Thus, the greatest common divisor of 78 and 127, $\gcd(78, 127)$, is 1.

$$\begin{aligned} \gcd(a, b) &= (a*x) + (b*y) \\ \gcd(78, 127) &= 1 = (78*57) + (127*-35) \\ &\Rightarrow x = 57,\ y = -35 \end{aligned}$$

Since

$$ax + by = 1$$

can be reduced modulo b to give

$$1 = ax \mod b$$

we also have a value for the multiplicative inverse of b modulo a, namely 57 which is the inverse of 78 modulo 127.