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 $K = (g^b)^a = (177147)^{17}$.
5. Bob computes the key $K = (g^b)^a = (129140163)^{11}$.
6. Both Alice and Bob now have the same key, $K = 16659986017630980004602663452498623354$-$817904066703829523539142428422125936921325414886738 7$

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 $\{0, \ldots, 22\}$.
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 $\{0, \ldots, 22\}$ 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

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

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 $\mathrm{e} \times \mathrm{d} \equiv 1 \mod (\phi)$.
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 $\mathbb{Z}_{34}$