CSC 591, Homework 2

Fatema Olia - 200253671
folia@ncsu.edu

October 15, 2018

1. The key exchange equations between Alice and Bob are as follows:
   1. $s = k \oplus r$
   2. $u = s \oplus t$
   3. $w = u \oplus r$

Bob outputs $val = w \oplus t$, this can be reduces as follows:
$val = u \oplus r \oplus t$ (From 3)
$val = s \oplus r$ (From 2)
$val = k$ (From 1)
Thus, Alice and Bob output the same key.

This scheme is not secure, it fails in the Secure Key Agreement game. In this scheme the adversary can see the transcript (s, u, w), and tell the difference between the actual key and a randomly selected one. The attack is as follows:

Adversary:
- Receive transcript (s, u, w) and a key k_b
- Calculate $w \oplus u = r$ (to get the value of r)
- Then calculate $s \oplus r = k$ (to get the value of k)
- If $k = k_b$ then output 1
- Else output 0

2. The scheme given, $\Pi(Gen, Enc, Dec)$, can be represented as follows:

Gen(x, h)
choose a uniform $x \in Z_q$ as the secret key
Calculate public key $h = g^x$

Enc(G, g, q, h, b)
choose a random $y \leftarrow Z_q$
$c_1 = g^y$
IF $b = 0$:
$c_2 = h^y$, where $h^y = g^{xy}$
IF $b = 1$:
choose a random $z \leftarrow Z_q$
$c_2 = g^z$
ciphertext is (c_1, c_2)

Dec(c_1, c_2, x, h)
calculate $k = c_1^x = g^{xy}$
IF $k = c_2$:
$b = 0$
ELSE:
$b = 1$

Thus, this scheme can efficiently decrypt the ciphertext given the private key x. We can prove the security of this scheme as follows:

Assumption:
1) The Diffie-Hellman assumption is true in G.
2) Towards a contradiction, assume $\exists A$ such that
$Pr[A_{wins} Pub_{\Pi}^{CPA}] = \frac{1}{2} + p(n)$

Reduction:
Consider an adversary A_{DDH} that tries to distinguish the Diffie-Hellman key agreement game, i.e. it outputs 0 if $Z = g^{xy}$ (where g^{xy} is the chosen key) or 1 if $Z = g^z$ (Where g^z is random). It can use A to try and win the distinguishing game. The algorithm would be as follows:

$A_{DDH}(G, g, q, X, Y, Z)$:
- Generate (G, g, q, h) as the public key for A (where $h = X$)
- A inputs two messages 0,1. These messages have to be either 0 or 1 since this scheme encrypts a single bit.
- Set $c_1 = Y$ and $c_2 = Z$ and send (c_1, c_2) to A.
- IF A outputs 0, then output 0.
- ELSE IF A outputs 1, then output 1.

Analysis:
In the reduction, the bit to be encrypted is effectively chosen by the A_{DDH} game's oracle. If $Z = g^{xy}$ then 0 is encrypted by the oracle, otherwise if $Z = g^z$ then 1 is encrypted by the oracle. Thus, the probability that A_{DDH} wins is same as the probability of A winning.

$$Pr[A_{DDH}wins] = Pr[A_{wins}Pub_{\Pi}^{CPA}] = \frac{1}{2} + p(n)$$

However, from our first assumption, A_{DDH} cannot win the key agreement game with a probability greater than $\frac{1}{2} + neg(n)$. Thus, our assumption about A must be incorrect. A cannot with the game with a probability of $\frac{1}{2} + p(n)$. Hence the encryption scheme is secure.

3. The adversary wishes to decrypt a message $c = m^e \bmod n$ intended for Alice. The adversary can query Alice with any ciphertext and receive the corresponding plain text (except c). The adversary knows (n, e) as that is the public key of Alice.
Suppose the adversary chooses a random message x.
The adversary can set $c' = c \,.\, x^e \bmod n$ and send this to Alice.
Alice will decrypt this as follows:
$m' = c'^d \bmod n$
$m' = (c \,.\, x^e)^d \bmod n$
$m' = c^d \,.\, x^{ed} \bmod n$
$m' = m^{ed} \,.\, x^{ed} \bmod n$ (Since $c = m^e \bmod n$)
We know that e, d are modular inverse in n.
Thus, $m' = m \,.\, x$
Alice will return m'.

Since the adversary knows the value of x, the adversary can get the value of m from m'.

4. For the RSA encryption scheme: $p = 11$, $q = 23$, $n = 253$, $e = 7$,
   $\Phi(n) = (p-1)(q-1) = 220$
   1. Using Extended Euclidian Algorithm to find Bob's private key d:
      Since $e = 7$, we have $7 * d \bmod 220 = 1$.
      Consider,
      1) $220 = 7(31) + 3$
      2) $7 = 3(2) + 1$
      3) Thus, from 2: $1 = 7 - 3(2)$
      4) From 1: $3 = 220 - 7(31)$
      Substituting 4 in 3:
      $1 = 7 - (220 - 7(31))2$
      $1 = 7 - (2(220) - 7(62))$
      $1 = 7 + 7(62) - (2(220) \bmod 220)$
      $1 = 7(63)$
      Thus 63 is the inverse of 7.
      $d = 63$
   2. The message to be sent by Alice is $m = 44$
      Alice will encrypt the message as follows:
      $c = m^e \bmod 220$
      $c = 44^7 \bmod 220$
      $\therefore c = 33$
   3. The cyphertext Bob receives is $c = 103$
      Bob will decrypt the message as follows:
      $m = c^d \bmod 220$
      $m = 103^{63} \bmod 220$
      $\therefore m = 130$
5. Bob receives two ElGamal ciphertexts from Alice - (B_1, C_1) and (B_2, C_2).
   For the ciphertexts, $B_i = g^{y_i}$ and $C_i = g^{xy_i} . m_i$. Public key is g^x.
   1. If $B_1 = B_2$:
      This means $g^{y_1} = g^{y_2}$, thus $y_1 = y_2$.
      Consider the ratio of C_1 and C_2:
      $$\frac{C_1}{C_2} = \frac{g^{xy_1} . m_1}{g^{xy_2} . m_2}$$

$$\frac{C_1}{C_2} = \frac{g^{xy_1} \cdot m_1}{g^{xy_1} \cdot m_2}$$
$$\therefore \frac{C_1}{C_2} = \frac{m_1}{m_2}$$

Thus, if we get even one of the messages it would be easy to find the other message.

2. If $B_1 = g \cdot B_2$:
   This means $g^{y_1} = g^{y_2+1}$, thus $y_1 = y_2 + 1$.
   Consider the ratio of C_1 and C_2:
$$\frac{C_1}{C_2} = \frac{g^{xy_1} \cdot m_1}{g^{xy_2} \cdot m_2}$$
$$\frac{C_1}{C_2} = \frac{g^{x(y_2+1)} \cdot m_1}{g^{xy_2} \cdot m_2}$$
$$\therefore \frac{C_1}{C_2} = \frac{g^{x} \cdot m_1}{m_2}$$
   Thus, if we get even one of the messages it would be easy to find the other message since g^x is a public key and is easily accessible by the adversary.
3. If $B_1 = (B_2)^2$:
   This means $g^{y_1} = g^{2y_2}$, thus $y_1 = 2y_2$.
   Consider the ratio of C_1 and C_2:
$$\frac{C_1}{C_2} = \frac{g^{xy_1} \cdot m_1}{g^{xy_2} \cdot m_2}$$
$$\frac{C_1}{C_2} = \frac{g^{2xy_2} \cdot m_1}{g^{xy_2} \cdot m_2}$$
$$\therefore \frac{C_1}{C_2} = \frac{g^{xy_2} \cdot m_1}{m_2}$$
   In this case we don't know the value of g^{xy_2} and it is difficult to find this value according to the Diffie-Hellman assumption. Thus, knowing anything about any of the messages does not give information about the other. This is scheme is secure.