Name Surname: ____________________ **Student #:____________**

CENG 471 CRYPTOGRAPHY
Midterm Exam, 03 May 2017

Exam duration is two hours.

Q.1) (25 points) The following authenticated key agreement protocol is given:

$$1: A \rightarrow B: \; g^{x}\, mod\, p$$
$$2: B \rightarrow A: \; g^{y}\, mod\, p, E_k(S_B(g^{y}\, mod\, p, g^{x}\, mod\, p)$$
$$3: A \rightarrow B: \; E_k(S_A(g^{x}\, mod\, p, g^{y}\, mod\, p)$$

We assume that the parties have agreed on a (g, p) pair (g is generator and p is prime number) for Diffie-Hellman key exchange, that each user has RSA keys for digital signatures and that they have agreed on a block cipher E for use in subsequent encryption. Furthermore, k is the agreed secret key and S_A and S_B denotes A: s and B: s signature operations, respectively.

Please describe the actions and knowledge of the parties after all three messages. The A and B as both ends of this protocol with the actions at receipt of messages 2 and 3, what beliefs they have at that stages. Are A and B successfully authenticated to each other after protocol run?

ANSWER 1)

(i) After receiving X as message 1, B can choose a y and compute $k = X^{y}\, mod\, p$ as the session key. He then computes $Y = g^{y}\, mod\, p$, $signs\ (Y, X)$ and encrypts it using key k. At this stage, B has no reason to believe that the received message was actually from A.

(ii) After receiving (Y, c) as message 2, A can compute $k = Y^{x}\, mod\, p$. Then k is the agreed common key, so she can use this to decrypt c, getting s. Finally, she verifies that s is B: s signature on (Y, X). A can know conclude that the sender of message 2 knows:

- k, since he could encrypt using it.
- B: s signing key, since could produce the signature s.
- X and y, the discrete log of Y (since A successfully decrypted c using $k = Y^{x}$, but anybody else could only have computed k as X^{y}).
- (Y, X), since he signed it; this knowledge must be recent, since it includes X, which A herself chose just before sending message 1.

From this evidence, A believes that the sender of message 2 is B and that therefore A and B share k.

(iii) After receiving c' as message 3, B decrypts it and verifies that the plaintext is A: s signature on (X, Y). From similar reasoning as above, B concludes that the sender of message 3 is A and that A and B share k.

Q.2) (20 points) Let $E_k(m), D_k(c)$ be a block cipher. Fischer S Mixer (FSM) mode encrypts a sequence of message blocks $m_1, m_2, \ldots$ by the sequence of ciphertext blocks $c_1, c_2, \ldots$ using the following method:

$$c_i = m_{i-1} \oplus E_k(m_i \oplus c_{i-1}), \qquad i \geq 1$$

m_0 and c_0 are fixed (public) initialization vectors.

a) Please describe how decryption is performed.

b) Suppose ciphertext block c_i is damaged in transmission. Which plaintext blocks become un-decipherable as a result? Please explain.

Name Surname: ____________________ **Student #:**____________

CENG 471 CRYPTOGRAPHY
Midterm Exam, 03 May 2017

Exam duration is two hours.

ANSWER 2)

a) XORing m_{i-1} to both sides of the encryption equation gives:

$$c_i \oplus m_{i-1} = E_k(m_i \oplus c_{i-1})$$

Applying the decryption function on both sides gives:

$$D_k(c_i \oplus m_{i-1}) = m_i \oplus c_{i-1}$$

So; $m_i = c_{i-1} \oplus D_k(c_i \oplus m_{i-1})$.

b) If c_i was damaged then m_i is damaged. If m_i is damaged then m_{i+1} is damaged. From then on all messages are damaged.

Q.3 (20 points) We consider the RSA encryption.

a) To illustrate the RSA system, we use primes $p = 23$ and $q = 17$. As public encryption key we use $e = 3$. Compute the decryption key d. Please show your computation steps.

b) Please describe in detail how the ciphertext $C = 165$ is decrypted and how the algorithm for efficient modular exponentiation works.

ANSWER 3.a)

We have that $n = 391$ *and* $\Phi(N) = (p-1)(q-1) = 352$. We compute d with the Extended Euclidean Algorithm and $d = 235$.

ANSWER 3.b)

To decrypt 165 means to compute 165^{235} *mod* 391.

i	2^i	165^{2^i}
0	1	165
1	2	165^2
……		

We use the algorithm for modular exponentiation. The number $(235)_{10} = (11101011)_2$ in binary form. So the final result is obtained by multiplying ($modulo$ 235) the number in the third column in rows with $i = 0,1,3,5,6,7$.

Q.4–optional for Q.5) (35 points)

a) (15 points) Explain how the Diffie-Hellman key agreement protocol works and what its purpose and main properties are. Give an example with p = 17 and g = 2 here p is prime and g is primitive element of Z_p.

b) (20 points) What is the man-in-the-middle attack on Diffie-Hellman? Give an example with p = 17, g = 2. Sketch one counter-measure against this attack.

ANSWER 4.a)

The Diffie-Hellman key agreement protocol establishes a shared key between two parties without any previous interaction. Two nice properties is that both parties contribute equally to the randomness in the shared secret, and once the randomness used in the protocols has been erased, no future compromises of the parties will compromise the shared key (so-called forward security).

Name Surname: ____________________ **Student #:____________**

CENG 471 CRYPTOGRAPHY
Midterm Exam, 03 May 2017

Exam duration is two hours.

The protocol has as shared, public parameters a prime p and an element g of order n. Party A chooses a number a randomly from {0, 1, . . . , n−1}, computes x = g^a mod p and sends x to party B. Party B chooses a number b randomly from {0, 1, . . . , n − 1}, computes y = g^b mod p and z = x^b mod p, erases b, and sends y to party A. Party A computes z = y^a mod p and erases a. A and B now share z.

With $p = 17$, $g = 2$:

$$\begin{tikzcd}
a \leftarrow 3 \arrow[rr, "8"] & & b \leftarrow 5 \\
x \leftarrow 2^3 \bmod 17 = 8 & & y \leftarrow 2^5 \bmod 17 = 15 \\
z \leftarrow 15^3 \bmod 17 = 9 & & z \leftarrow 8^5 \bmod 17 = 9 \arrow[ll, "15"']
\end{tikzcd}$$

ANSWER 4.b)

The man-in-the-middle attack on Diffie-Hellman is possible since there is no authentication in Diffie-Hellman. Party A cannot know if the message y comes from party B or from some other attacker. Party E simply inserts himself in the middle of the protocol, pretending to be party B to party A, and party A to party B, running two copies of the Diffie-Hellman protocol:

$$\begin{tikzcd}
 & a' \leftarrow 7,\ b' \leftarrow 4 & \\
a \leftarrow 3 \arrow[r, "8"] & x' \leftarrow 2^7 \bmod 17 = 9 \arrow[r, "9"] & b \leftarrow 5 \\
x \leftarrow 8 & y' \leftarrow 2^4 \bmod 17 = 16 & y \leftarrow 15 \\
z_A \leftarrow 16 & z_A \leftarrow 8^4 \bmod 17 = 16 \arrow[l, "16"'] & z_B \leftarrow 8 \arrow[l, "15"'] \\
 & z_B \leftarrow 15^7 \bmod 17 = 8 &
\end{tikzcd}$$

One simple counter-measure against this attack is for each party to sign the messages in the protocol.

Q.5 –optional for Q.4) (35 points) Alice wants to send an encrypted message to Bob using RSA, but doesn't know his public key. So, she sends Bob an email asking for the key. Bob replies with his RSA public key (e, N). However, the active adversary intercepts the message and changes one bit in e from 0 to 1, so Alice receives an email claiming that Bobs public key is (e', N), where e' differs from e in one bit. Alice encrypts m with this key and sends it to Bob. Of course, Bob cannot decrypt, since the message was encrypted with the wrong key. So he resends his key and asks Alice to send the encrypted message again, which she does. The adversary eavesdrops to the whole communication without interfering further. Describe how adversary can now recover m.

ANSWER 5)

The adversary has eavesdropped and thus knows $c = m^e$ and $c' = m^{e'}$. He also knows that e and e' furthermore, $\gcd(e, e') = 1$. So the adversary can find integers x and y such that

$$ex + e'y = 1\,.$$

Hence,

$$c^x . c'^y = m^{ex+e'y} = m\,.$$