Name Surname: _____ **Student #:_____**

CENG 471 CRYPTOGRAPHY
Final Exam, 01 June 2018
ANSWERS

Exam duration is two hours.

Q.1 (30 points)
a) (15 points) Given are two protocols in which the sender's party performs the following operation. Please explain that which steps have to be done by the receiver for each A and B protocols?

Protocol A:

$$y = e_{k_1}(x||H(k_2||x))$$

where x is the message, H is a hash function such as SHA-1, e is a symmetric-key encryption algorithm, "||" denotes simple concatenation, and k_1, k_2 are secret keys which are only known to the sender and the receiver.

Protocol B:

$$y = e_k(x||sig_{k_{pr}}(H(x)))$$

where k is a shared secret key, and k_{pr} is a private key of the sender (not shared with the receiver). Provide a step-by-step description (e.g., with an itemized list) of what the receiver does upon reception of y.

b) (15 points) Evaluate the following security services for each given protocol A and B:

- confidentiality
- integrity
- non-repudiation (preventing an entity from denying previous commitments or actions)

Answer:

a)

Protocol A performs the following:

1. Decryption of y using symmetric key k_1

$$d_{k_1}(y) = x||H(k_2||x)$$

2. Concatenate, k_2 and x, where k_2 is second secret key already shared between sender and receiver.
3. Compute hash of $k_2||x$, that is $H(k_2||x)$.
4. Compare computed hash value with the one obtained in step 1. If they are identical then the receiver can be sure that the integrity of received message.

Protocol B performs the following:

1. Decrypt as in step 1 of Protocol A; $d_k(y) = x||sig_{k_{pr}}(H(x))$ using shared symmetric key k.
2. Compute $H(x)$
3. Feed $H(x)$ and $sig_{k_{pr}}(H(x))$ into verification algorithm, check if signature on $H(x)$ is valid. Verification algorithm needs public key of the sender.

Name Surname: _____ **Student #:_____**

CENG 471 CRYPTOGRAPHY
Final Exam, 01 June 2018
ANSWERS

Exam duration is two hours.

b) For protocol A we have:

- confidentiality, YES through encryption
- integrity, YES through hashing; changing y lead to invalid pair x' and $H(k_2||x')$.
- non-repudiation, NO, both Alice (sender) and Bob (receiver) can generate valid message:

$$y = e_{k_1}(x||H(k_2||x)$$

For protocol B we have:

- confidentiality, YES through encryption
- integrity, YES through signing; changing y lead to invalid pair x' and $sig_{k_{pr}}H(x'))$
- non-repudiation, YES, only sender can send a message with valid signature.

Q.2 (30 points)

a) **(15 points)** Alice's ElGamal public key is $(p, \alpha, \beta) = (17,3,6)$. Bob is confused which of two different ElGamal signatures (without hash) for the message *m = 12* he wrote down is the correct one: one of these possible signatures has appendix *(r, s) = (13, 7),* the other *(r, s) = (12, 8).* Check which of them is the valid signature. $(Hint: v_1 \equiv \beta^r r^s, v_2 \equiv \alpha^m \ mod\ p)$

b) **(15 points)** Suppose a second message m' = 7 is signed with signature (r', s') = (12, 15). Find (together with the knowledge from the first part) the secret integer k.

$$(\ Hint:\ In\ the\ ElGamal\ signature\ scheme,\quad s \equiv k^{-1}(m - a.r)\ mod\ p - 1\ \ )$$

Answer:

a) Alice's ElGamal public key is $(p, \alpha, \beta) = (17,3,6)$.

Bob is confused which of two different ElGamal signature (without hash) for the message *m = 12.* He wrote down is the correct one between *(r, s) = (13, 7)* and the other *(r, s) = (12, 8)*:

$$v_1 \equiv \beta^r r^s, v_2 \equiv \alpha^m \ mod\ p)$$

So, lets first calculate $v_2 \equiv \alpha^m \ mod\ p = \ 3^{12}\ mod\ 17 \equiv 4\ mod\ 17$

Second lets calculate $v_1 \equiv \beta^r r^s$ for both options, which one is equal to v_1, hence we will be found correct answer.

$for\ (r,s) = (13,7)\ ;\ v_1 \equiv \beta^r r^s = \ 6^{13}13^7 \equiv 6\ mod\ 17$ and $v_1 \neq v_2$, which is not correct signature.

$for\ (r,s) = (12,8)\ ;\ v_1 \equiv \beta^r r^s = \ 6^{12}12^8 \equiv 4\ mod\ 17$ and $v_1 = v_2$, which is correct signature.

In your answer you can use successive squaring method to calculate exponentiations.

b) Suppose a second message *m' = 7* is signed with signature *(r', s') = (12, 15).* Find (together with the knowledge from the first part) the secret integer *k*.

$$(\ Hint:\ In\ the\ ElGamal\ signature\ scheme,\quad s \equiv k^{-1}(m - a.r)\ mod\ p - 1\ \ )$$

Let $(r,s) = (12,8)\ and\ (r',s') = (12,15).\ Since\ r = r', the\ same\ k\ was\ used\ for\ both\ signatures.$
We get;

$$sk - m \equiv -ar \equiv s'k - m'\ \ mod\ p - 1$$

Name Surname: _____ **Student #:_____**

CENG 471 CRYPTOGRAPHY
Final Exam, 01 June 2018
ANSWERS

Exam duration is two hours.

Therefore

$$(s - s')k \equiv m - m' \; mod \; p - 1$$

That is

$$(-7)k \equiv 5 \; mod \; 16$$

Now, $\gcd(-7,16) = 1$, and (with the Extended Euclidean algorithm) we get

$$k \equiv (-7)^{-1}.5 \equiv 13 \; mod \; 16$$

Q.3 (20 points) Assume the RSA public key is given by $(n, e) = (527,11)$.

a) **(10 points)** Determine the corresponding RSA private key.
b) **(10 points)** Explain how RSA encryption and decryption works in general. Compute the encryption of the message m = 3.

Answer:

a) One finds (e.g. with Fermat's factorization method) that 527 = 17 · 31 is the prime factorization

of n = 527. So let p = 17 and q = 31. Then ϕ(n) = (p− 1) · (q− 1) = 16 · 30 = 480.
Find d with $d.e \equiv 1 \; mod \; 480$ with the extended Euclidean algorithm:

480 = 43.11 + 7
11 = 1. 7 + 4
7 = 1. 4 + 3
4 = 1. 3 +1

So;

1= 4 -**3** and 3 = 7 – 1.4

1 = 4 – 1.(7 – 1.4)= 4 – 1.7 – 1.4 =

4= 11 – 1.7 ➔ 2.**4** – 1.7= 2.(11 – 1.7) – 1.7=1

2.11 – 3.7 = 1

7 = 480 – 43.11 ➔

2.11 – 3.(480 – 43.11) = 1

131.11 – 3.480 = 1

We see that d = 131 is the solution, and (n, d) = (527, 131) is the private key.

b) Explain how RSA encryption and decryption works in general. Compute the encryption of the message m = 3.

(n, e) is the public key, (n, d) the private (secret) key. Here, n = p.q is a product of two distinct primes p and q, and e is chosen such that $gcd(e, \phi(n)) = 1$. Here, $\phi(n) = (p - 1) \cdot (q - 1)$. Moreover, d satisfies the condition $e.d = 1 \; mod \; (p - 1)(q - 1)$. If m is (the plaintext of) the message (given as a positive integer), then $c = m^e \; mod \; n$ is the corresponding ciphertext. To decrypt, calculate $c^d \; mod \; n$, which gives back m.

In the example: $m^e = 3^{11} = 3^{8+2+1} = 3^8 3^2 3^1$. We have $3^1 = 3 \bmod 527$, $3^2 = 9 \bmod 527$,

Name Surname: _____ **Student #:_____**

CENG 471 CRYPTOGRAPHY
Final Exam, 01 June 2018
ANSWERS

Exam duration is two hours.

$3^4 = 9 \cdot 9 = 81 \bmod 527$, $3^8 = 81 \cdot 81 = 6561 = 237 \bmod 527$.

Hence $3^{11} = 3 \cdot 9 \cdot 237 = 75 \bmod 527$.
The result is c = 75.

Q.4 (20 points)

a) **(10 points)** Please explain that why longer key sizes are preferred in RSA then DES or AES?

Answer: RSA, Diffie-Hellman, and other asymmetric algorithms use larger keys than their symmetric counterparts. Common key sizes include 1024 bits and 2048 bits. The keys are this large because factoring, while still a difficult operation, is much easier to perform than the exhaustive key search approach used with symmetric algorithms. The slowness of asymmetrical systems is also due to the larger key sizes. Since most computers can only handle 32 or 64 bits precision, different "tricks" are required to emulate the 1024 bit and 2048 bit integers. However, the additional processing time is justified, since, for security purposes, 2048 bit keys are considered more secure.

b) **(10 points)** Please listed main security functions with short descriptions and explain that which cryptographic tools satisfy which security functions.

Answer: The security functions with short descriptions are listed hereunder with the names of related cryptographic tools.

Confidentiality; which means hiding of information from non-legitimate entities. For this purpose; we mostly prefer to use symmetrical cryptosystems i.e. DES, AES. But, we also can use asymmetrical cryptosystems for confidentiality for short texts, because its' algorithms have high computational cost.

Integrity checking; we have to be sure that received message has not any alteration since send by receiver. For this purpose; hashing functions, MAC (message authentication code), digital signature solutions can be used.

Non-Repudiation (Identification, Authentication); In Internet (or virtual world), persons should not deny their actions such as their orders at virtual market. For this purpose; asymmetrical cryptosystems with the support of PKI (Public Key Infrastructure) and CA (certification authorities – trusted third parties) define solution schemes to identify sender and receiver sides.