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

CENG 471 CRYPTOGRAPHY
Final Exam, 14 June 2017

Exam duration is two hours.

Q.1) (30 points) Explain your answer with few sentences for the following questions:

a) **(5 points)** When a cryptographic construction provides message authenticity, what does the receiver learn?
answer: Authenticity enables the receiver to verify the identity of the sender of the message, implying the message's integrity.

b) **(5 points)** What is the integrity and which cryptographic tools can be used to satisfy its requirement?
answer: Hashing functions are used with digital signature algorithms.

c) **(5 points)** Shall we use symmetrical cryptosystems to satisfy integrity and why?
answer: No, because symmetrical cryptosystems can satisfy only secrecy (confidentiality).

d) **(5 points)** What is the CA and its role in the trust model of a PKI system?
answer: CA is trusted to verify the mapping between public keys and identities. CA is trusted to protect its private key from being leaked. The user must trust her machine to protect the generation and use of her private key.

e) **(5 points)** How does a private key signature ensure non-repudiability?
answer: Private key can only belong to signer, and signing the hash ensures that the message's integrity can be associated with the private key encryption.

f) **(5 points)** What is the main drawback of the one-time pad cryptosystem?
answer: The one time pad system requires that we secretly communicate in advance a key which is at least as long as the message we will send. This is a severe practical difficulty since it requires substantial secret communication in advance of the desired secret communication.

Q.2) (25 points) Alice is the owner of a company. In a new public key encryption scheme (known as ElGamal's encryption scheme), Alice randomly selects her private decryption key x (where x is an integer such that $1 \leq x \leq (p-1)$ and computes her public key $\mathrm{a} = g^x \ (mod\ p)$, where p is a large prime and g is a publicly known generator of Z_p^*. Z_p^* is the set of non-negative integers below p that are relatively prime to p.

Encryption: To encrypt a message $\in Z_p^*$; Bob first picks a random integer $1 \leq k \leq (p-1)$ such that $\gcd(k, p-1) = 1$ and obtains Alice's public key y. Next Bob computes $r = g^k \ (mod\ p)$ and $s = my^k (mod\ p)$ and sends $C = (r, s)$ as the ciphertext.

Decryption: Alice decrypts the ciphertext (r, s) as follows: She computes $r' = r^x (mod\ p)$ and then computes t such that $r'.t \equiv 1\ (mod\ p)$. She recovers m by computing $st\ (mod\ p)$.

Show that how does the computation $st\ (mod\ p)$ indeed recover m.

ANSWER 2)

Encryption:

$$y = g^x\ (mod\ p),\ \ r = g^k (mod\ p), \qquad s = m.y^k = m.g^{xk} (mod\ p)\ and\ C = (r, s)$$

Decryption:

$$r' = r^x = g^{xk} (mod\ p)\ and\ r't \equiv 1 (mod\ p) means\ that\ t = g^{-(xk)}$$

t is the multiplicative invers of r'.

$$m = s.t(mod\ p) = m.g^{xk}.g^{-(xk)}\ (mod\ p) = m$$
Because; $g^{xk}.g^{-(xk)}\ (mod\ p) = 1$

Q.3 (20 points) Alice has a public key *n*=33, *e*=13. Bob uses it to encrypt his plain text.

a) The plain text is 6, what is the cipher text?
b) What is Alice’s private key *d*?
c) Explain why Alice’s public/private key pair is weak, and how to choose a public key that makes RSA more secure?

ANSWER 3.

a) $\boldsymbol{C = m^e\ mod\ n}$ **This gives the ciphertext for plaintext 6. Here;** $\boldsymbol{C = 6^{13}\ mod\ 33.}$ **Which is calculated by successive squaring method.**

$$\boldsymbol{(13)_{10} = (1101)_2}$$
$$\boldsymbol{6^1.6^4.6^8 = 6^{13}}$$
$$\boldsymbol{6^2 \equiv 36\ \equiv 3\ mod\ 33}$$
$$\boldsymbol{6^{2^2} = 6^4 = 3^2 \equiv 9\ mod\ 33}$$
$$\boldsymbol{6^8 = 9^2 = 81 \equiv 15\ mod\ 33}$$

So, the result is $\boldsymbol{C = 6.9.15\ mod\ 33 = 18}$

b) $\boldsymbol{n = 33\ so\ p = 3\ and\ q = 11\ are\ prime\ numbers.}$

$$\boldsymbol{\Phi = (p-1).(q-1) = 2.10 = 20}$$
$$\boldsymbol{\gcd(e,\Phi) = 1\ \text{rule is satisfied with}\ \gcd(13,20) = 1}$$

$\boldsymbol{e.d \equiv 1\ mod\ 20}$ **and** $\boldsymbol{13.d \equiv 1\ mod\ 20}$ **via Extended Euclid’s Algorithm** $\boldsymbol{d = 17}$

c) **p and q** are selected primes should be large (big integers, i.e. 2048 bits length). And their sizes should be close.

Q.4) (10 points) Use the extended Euclidean algorithm to compute the greatest common divisor d of 654 and 123 and to find integers m and n such that $654m + 123n = d$.

ANSWER 4. We have

$$654 = 5 \cdot 123 + 39$$
$$123 = 3 \cdot 39 + 6$$
$$39 = 6 \cdot 6 + 3$$
$$6 = 2 \cdot 3 + 0$$

and so the gcd $d = 3$. Working backwards, we have

$$3 = 39 - 6 \cdot 6$$

$$= 39 - 6(123 - 3 \cdot 39) = 19 \cdot 39 - 6 \cdot 123$$

$$= 19(654 - 5 \cdot 123) - 6 \cdot 123 = 19 \cdot 654 - 101 \cdot 123$$

and so $m = 19$ and $n = -101$.

Q.5) (15 points) Why key distribution is a hard problem and how does it work PKI infrastructure to satisfy key distribution efficient way? For instance; how can you trust that a signature of a message is really belong to sender?

Answer 5) Under Internet platform and created virtual world, the secure operations and communication are basic requirements. To satisfy them, we need crypto solutions for special protocols. Each of these crypto solutions require entity (user or program or device) specific key generation and sharing. There are plenty of entities in virtual world. How can we do this job and how can we be sure about the identity of the other side? To solve related key generation, distribution and identification problems, PKI infrastructure define very popular and strong platform. Under PKI infrastructure a trust model works among certification authorities – CAs. Each member of the system have to generate own public and private key pair and contact with CA with own identity documents. CA knows only public key and owner's identity information and take registration of new member and prepared a certification. This certificate is prepared at X509 standard and signed by CA. So; when we receive a signed message, we can verify signature for message and its certificate separately. By this way we can sure the identity of the message owner. We can also check the certificate directly from CA's directory list to check that this certificate is in revocation list or not.