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

CENG 471 CRYPTOGRAPHY
Midterm-2 Exam, 04 May 2018

Exam duration is two hours.

Q.1 (20 points) Please give the descriptions of the following terms:

a) (10 points) HASH function can be used a cryptosystem? Please define the specifications of a cryptosystem and list main specifications of a Hash function.

Answer: Hash function cannot be used a cryptosystem, because it generates a fixed length digest (fingerprint) for any size of message. And it has one-way property, means that we cannot regenerate original message from its hash result. To be a cryptosystem; it should include key generation, encryption and decryption schemes.

b) (10 points) How it works Certification Authority (CA) and X.509 certificate for identification purpose?

Answer: CA approves the relation of person's public key and his/her identity by a certification. CA also signs this certificate by own private key. By this way, anyone can verify it by public key of CA. The certificate has to includes certificate number, validate time interval, owner identity information etc. according to X509 standard.

Q.2 (20 points)

a) (10 points) Why is the usage of prime numbers and modular arithmetic is important for asymmetrical cryptography? Please give the reasons clearly.

Answer: Asymmetrical Cryptographic schemes are implemented by integer numbers and arithmetic operations. But, for encryption and decryption operations have to be done on finite integer number sets. This finite integer numbers have to have to be field property. For this, it should support addition and multiplication arithmetic operations. Therefore, modular arithmetic turns infinite integer number set to a finite number set as a set of residue classes. Which is represented by Z_p**.** Here, p is chosen a prime number. Because, each element of Z_p should have its inverse for both addition and multiplication. To guarantee that, each element of Z_p has to be relatively prime with p and if p is prime, this rule certainly satisfied. Because prime numbers have only two divisors which are 1 and p.

b) (10 points) What is the importance of "one-way trap function" to build a cryptosystem? Could you explain with an example?

Answer: The plaintext is turned to cipher text by an encryption function (f), and this operation should be easily and efficiently implement. Anyone can do encryption of a message before sending. But, the cipher text should not be decrypted by a decryption function which is the reverse of f and represent as f^{-1}. But, this reverse function should be hard for un-legitimate receivers and easy for legitimate users. To satisfy this requirement, the key should be used with function f and f^{-1}. Here, key has a trap role for decryption time. Due that reason, to have a "one-way trap function" is important to build a cryptosystem. For example; in ElGamal – there is a private-public key pair exist. When a sender encrypts a message with receiver public key, which is an easy operation. But, without private key; the receiver cannot decrypt the message. The private key has a trap role. Due that reason, if the receiver has private key; decryption is an easy operation.

Q.3) (20 points) Please find the value of x to satisfy the given congruencies concurrently;

$$x \equiv 1 \ (mod\ 3)$$
$$x \equiv 3 \ (mod\ 7)$$
$$x \equiv 5 \ (mod\ 11)$$

Name Surname: ____________________ **Student #:**_____________

CENG 471 CRYPTOGRAPHY
Midterm-2 Exam, 04 May 2018

Exam duration is two hours.

Answer: $m = m1.m2.m3 = 3.7.11 = 231$

$$M1 = \frac{m}{m1} = \frac{231}{3} = 77$$
$$M2 = \frac{m}{m2} = \frac{231}{7} = 33$$
$$M3 = \frac{m}{m3} = \frac{231}{11} = 21$$
$$M1' = 77^{-1} \equiv 2\, mod\ 3$$
$$M2' = 33^{-1} \equiv 3\, mod\ 7$$
$$M3' = 21^{-1} \equiv 10\, mod\ 11$$
$$x = 1.77.2 + 3.33.3 + 5.21.10 = 154 + 297 + 1050 = 115\ mod 231$$

Q.4) (10 points) Please find the generator for Z_{13}? What is the specification of the generator for the asymmetrical cryptosystems?

Answer: p=13 and p-1 =12 and its multipliers are 4,3, and 2. So; let check that can be 2 a generator:

$$2^{\frac{12}{4}} \equiv 8\, mod\ 13$$
$$2^{\frac{12}{3}} \equiv 16 \equiv 3\, mod\ 13$$
$$2^{\frac{12}{2}} \equiv 64 \equiv 12\, mod\ 13$$

For all multipliers the test results are different from 1, therefore 2 can be a generator for Z_{13} finite field. In asymmetrical cryptosystems require finite fields and the generator number has a capability to generate all numbers under selected finite field. Hence, for arithmetic operations can be done by any number of the field, otherwise the usable number of elements of the field is less than the real size of the finite field.

Q.5) (20 points) As a prime number you selected p=13 and found the generator (g) from previous Q.4. Please try to generate a common secret key between Alice and Bob.

Answer:

First, both parties Alice and Bob have to build their private and public keys: To do that both parties select randomly their private keys $1 \leq Xa\ and\ Xb \leq p - 1$

$$Alice\ private\ key\ is\ Xa,$$
$Alice\ public\ key\ PUa = g^{Xa} mod\ p$

$$Bob\ private\ key\ is\ Xb,$$
$Bob\ public\ key\ PUb = g^{Xb} mod\ p$

Alice and Bob, send their public keys to each other via unsecure network i.e. Internet.

Both parties can generate common key:

$$Alice\ ;\ K_{common} = PUb^{Xa} mod\ p = (g^{Xb})^{Xa} = g^{Xa.Xb}\ mod\ p$$
$$Bob\ \ ;\ K_{common} = PUa^{Xb} mod\ p = (g^{Xa})^{Xb} = g^{Xa.Xb}\ mod\ p$$

Q.6) (10 points) We know the details of ElGamal digital signature to sign and to verify a signature on a message as given below. Please show that how it works the verification of digital signature with details.

Alice signs a message M to Bob by computing

–the hash $m = H(M)$, 0 <= m <= (q-1)

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

CENG 471 CRYPTOGRAPHY
Midterm-2 Exam, 04 May 2018

Exam duration is two hours.

–chose random integer K with 1 <= K <= (q-1) and gcd(K, q-1)=1

–compute temporary key: S1 = a^k mod q

–compute K^{-1} the inverse of K mod (q-1)

–compute the value: $S_2 = K^{-1}(m-x^A S_1)$ mod (q-1)

–signature is:(S_1,S_2)

any user B can verify the signature by computing

–$V_1 = a^m$ mod q

–$V_2 = {y_A}^{S1} {S_1}^{S2}$ mod q

–signature is valid if $V_1 = V_2$

Answer:

$$V_2 = {y_A}^{a^k}.a^{K^{K^{-1}.(m-x^A.S_1)}} = (a^{x_a})^{a^k}.a^{(m-x^A a^k)} = a^m.a^{x^A.a^k}.a^{-x^A.a^k} = a^m = V_1$$