CENG471 CRYPTOGRAPHY
Midterm – 2 16 Dec. 2022
2022 Fall
Q & A

Student Name and Number: ____________________

Q.1) (25 points)

- **a) (5 points)** Symmetric cryptosystems uses **substitution** and **permutation** methods for encryption.
- **b) (5 points)** Asymmetrical cryptosystems uses **one-way** and **trap** functions for encryption.
- **c) (5 points)** To have non-repudiation facility for your application, you have to use one of the **digital signature** cryptographic solution.
- **d) (10 points)** To receive my messages in secrecy from anyone at any time, I have to use **asymmetrical cryptographic** solutions, and they have to know **my public key** Hence, anyone, at any anytime, can send me a secret message by encrypted with **my public key** and I can read these messages by decrypted with **my private key.**

Q.2) (25 points) Please explain;

- **a) (10 points)** What are the domain parameters for an asymmetrical cryptosystem? For example, please discuss for ElGamal cryptosystem.

Answer:

Domain parameters should be public and should be known by the use of this crypto solution. For the ElGamal crypto solution, p is a prime number, and its g generator (or primitive number) is announced as domain parameters. Users of this ElGamal crypto solution, according to these domain parameters, generate their public and private key pairs.

- **b) (15 points)** Why prime numbers are mostly preferred to build an asymmetrical cryptosystem. (Hint: Please remember mathematical topics and their relations to build.)

Answer:

Asymmetrical crypto solutions use mathematical problems, and four arithmetic operations should be done properly. Mostly integer numbers are used with congruencies such as
Z_n^* ; $defines\ a\ multiplicative\ finite\ group\ with\ modulus\ n.$

The selected congruent number is n; if it is a prime number, then we ensure that all numbers between 1 and (n-1) are always relatively prime with n. Hence, we ensure that from 1 to n all numbers have own multiplicative inverses, and division is supported in this way. All other arithmetic operations such as addition, subtraction and multiplication are also supported naturally.

Q.3) (30 points) Please calculate and explain your steps for:

- **a) (15 points)** $7^{126382}\ (mod\ 15) = ?$

Answer:

CENG471 CRYPTOGRAPHY
Midterm – 2   16 Dec. 2022
2022 Fall
Q & A

Student Name and Number: ____________________

$$\mathrm{n} = \mathrm{p.q} \text{ then } 15 = 3.5 \; and \; \Phi(n) = (p-1).(q-1)$$

$$\Phi(15) = (3-1).(5-1) = 2.4 = 8$$

The power of 7 is 126382 can be reduced to smaller number as: 126382 $(mod\ 8)$= 6

Now, we have to find the result of $7^6 = 7^4.7^2\ (mod\ 15)$ by repeated squaring method:

$$7^2 = 49\ (mod\ 15) = 4$$

$$(7^2)^2 = 4^2\ (mod\ 15) = 1$$

$$7^6 = 1.4\ (mod\ 15) = 4$$

Hence; $7^{126382}\ (mod\ 15) = \ 4$

b) **(15 points)** Please use Chinese Remainder Theorem to find the x value:

$$x \equiv 3\ (mod\ 7)$$
$$x \equiv 1\ (mod\ 3)$$
$$x \equiv 2\ (mod\ 11)$$

Answer:

$$m = m_1.m_2.m_3 = 7.3.11 = 231$$

$$M_1 = m/m_1 = 231/7 = 33$$

$$M_2 = m/m_2 = 231/3 = 77$$

$$M_3 = m/m_3 = 231/11 = 21$$

$$M_1^{-1} = 33^{-1}\ (mod\ 7) = 5^{-1}\ (mod\ 7)\ and\ 5.2 \equiv 1\ (mod\ 7)\ hence\ M_1^{-1} = 2\ (mod\ 7)$$

$$M_2^{-1} = 77^{-1}\ (mod\ 3) = 2^{-1}\ (mod\ 3)\ and\ 2.2 \equiv 1\ (mod\ 3)\ hence\ M_2^{-1} = 2\ (mod\ 3)$$

$$M_3^{-1} = 21^{-1}\ (mod\ 11) = 10^{-1}\ (mod\ 11)\ and\ 10.10 \equiv 1\ (mod\ 11)\ hence\ M_3^{-1} = 10\ (mod\ 11)$$

$$x = a_1.M_1.M_1^{-1} + a_2.M_2.M_2^{-1} + a_3.M_3.M_3^{-1}\ (mod\ m)$$

$$x = (3.33.2 + 1.77.2 + 2.21.10)\ (mod\ 231)$$

$$x = (297 + 154 + 420)(mod\ 231)\ \equiv (66 + 154 + 189)(mod\ 231) \equiv 178\ (mod\ 231)$$

And
$178 \equiv 3\ (mod\ 7)$
$178 \equiv 1\ (mod\ 3)$
$178 \equiv 2\ (mod\ 11)$.

Q.4) (20 points) We are building a RSA cryptosystem with p=5 and q=11 primes.

CENG471 CRYPTOGRAPHY
Midterm – 2   16 Dec. 2022
2022 Fall
Q & A

Student Name and Number: ____________________

a) **(10 points)** If the public key is selected e=27, what should be the private key d=?
b) **(10 points)** M=3 as your message. Please encrypt and then decrypt it with RSA public and private keys.

(For your arithmetic operations, please use practical mathematical methods as learn in your lectures.)

Answer:

$$n = p.q = 5.11 = 55$$

$$\Phi(n) = (p-1)(q-1) = 4.10 = 40$$

$$\gcd(27,40) = 1 \; hence\ we\ can\ find\ d\ and\ d.e \equiv 1\ (mod\ 40)\ and\ 3.27\ \equiv 1\ (mod\ 40)$$

$$Public\ key\ (n,e) = (55,27)$$

$$Private\ key\ (n,d) = (55,3)$$

$$C = M^e\ (mod\ n) =\ 3^{27}\ (mod\ 55)$$

Repeated squaring is used for easy exponentiation, and 27 = 16 + 8 +2 + 1

$$3^2 = 9\ (mod\ 55)$$

$$3^4 = (3^2)^2 = 9^2 = 81 \equiv 26\ (mod\ 55)$$

$$3^8 = (3^4)^2 = 26^2 = 676 \equiv 16\ (mod\ 55)$$

$$3^{16} = (3^8)^2 = 16^2 = 256 \equiv 36\ (mod\ 55)$$

$$3^{27}\ (mod\ 55) = 3^{16}.3^8.3^2.3 = 36.16.9.3\ (mod55) = 42$$

$$C = 42$$

For the decryption of C is

$$M = C^d\ (mod\ n) = 42^3\ (mod\ 55) = 42^2.42 = 1764.42\ (mod55) = 4.42 = 168\ (mod\ 55) \equiv 3$$