Question 1 (1 mark)

What is a trapdoor one-way function?

Suggested answer:

Trapdoor one-way functions are a family of invertible functions f_k such that Y = $f_k(X)$ is easy if k and X known, X = $f_k(Y)$ is easy if k and Y are known, and $X = f^{-1}(Y)$ is infeasible if Y is known but k is not known.

Question 2 (1 mark)

Define what a Message Authentication Code (MAC) system is and the properties it should have.

Suggested answer:

A MAC system is a cryptographic system that generates a short piece of information known as checksum or authentication tag used to authenticate a message. A MAC is generated by a function $C_k(m)$ that can be computed by anyone knowing the secret key k.

The required security property is that, even with access to a large number of (message,MAC) pairs, it should be infeasible to compute a pair consisting of a new message and its MAC without knowledge of the secret key.

Question 3 (1 mark)

What are the roles of the public and private key?

Suggested answer:

In a public-key cryptosystem, a user's private key is kept private and known only to the user while the user's public key is made available to others to use. The private key can be used to encrypt a signature that can be verified by anyone with the public key in a signature scheme. When used as an encryption scheme, the public key can be used to encrypt information that can only be decrypted by the possessor of the private key.

Question 4 (2 marks)

The weakness of substitution cipher is the small key space. Alice decides to improve the security on the Caesar cipher by making the key space larger. She keeps the message $m = c = \{0, \cdots, 25\}$ as its original algorithm, but she increases the key space $k = \{0, \cdots, 49\}$ and defines a new cipher as follow:

$$E_k(m) = (k + m) mod\ 26$$

What is the security of Alice's new cipher as compared with the ordinary Caesar cipher? Justify your answers.

Suggested solution:

Alice's new cipher has a less secure security than the ordinary Caesar cipher. This is because $E_k(m) = E_{k\ mod\ 26}(m)$ for any k, the larger key space does not actually increase the number of possible encryption functions, but it does alter their distribution. Now the keys $\{0, \cdots, 23\}$ and $\{26, \cdots, 49\}$ are overlapping, and hence $E_0(), \cdots, E_{23}()$ and $E_{26}(), \cdots, E_{49}()$ have similar ciphertext. This actually increase the likely hood that $E_0(), \cdots, E_{23}()$ are twice as likely to be chosen $E_{24}()\ and\ E_{25}()$. In other words, the probability distribution is not uniformly distributed. An attacker can now get this statistical information to guess the message m.

Question 5 (4 marks)

Compute the following by demonstrating the step-by-step calculation correctly.

(i) Compute $21^{221} mod\ 123$ using fast exponentiation algorithm discussed in lecture and/or tutorial. Show all steps.
(ii) Compute $3037^{-1} mod\ 4051$
(iii) Use Euclid's algorithm to find integers x and y such that 25x + 41y = 1.
(iv) Find x such that the equation 18x = 11 mod 19 is satisfied?

Suggested answer:

(i) 21^{221} mod 123 = 21 mod 123 = 21.

The student is expected to use fast exponentiation to compute.

221 (in decimal) = 11011101 (in binary)

	2^7= 128	2^6= 64	2^5= 32	2^4= 16	2^3= 8	2^2= 4	2^1= 2	2^0= 1
221 =	1	1	0	1	1	1	0	1
21^{221} mod 123	21^{128} mod 123	21^{64} mod 123		21^{16} mod 123	21^{8} mod 123	21^{4} mod 123		21^{1} mod 123

	78 mod 123	**18 mod 123**	51 mod 123	**57 mod 123**	**78 mod 123**	**18 mod 123**	72 mod 123	**21 mod 123**
	19^{221} mod 123 = 78 × 18 × 57 × 78 × 18 × 21 mod 123 = **21 mod 123**							

$Thus\ 21^{221} mod\ 123 = 21\ mod\ 123 = 21.$

(ii) Compute 3221^{-1} mod 4019.

Suggested answer:

$3037^{-1} mod\ 4051 = -811\ mod\ 4051 = 3240$
The student is expected to use Extended Euclidean Algorithm to compute as follow:

n1	n2	r	q	a1	b1	a2	b2	a2'	b2'
4051	3037	1014	1	1	0	0	1	0	1
3037	1014	1009	2	0	1	1	-1	1	4050
1014	1009	5	1	1	-1	-2	3	4049	3
1009	5	4	201	-2	3	3	-4	3	4047
5	4	1	1	3	-4	-605	807	3446	807
4	1	0	4	-605	807	608	-811	608	3240

(iii) The student is expected to use Extended Euclidean Algorithm to compute as follow:

n1	n2	r	q	a1	b1	a2	b2
41	25	16	1	1	0	0	1
25	16	9	1	0	1	1	-1
16	9	7	1	1	-1	-1	2
9	7	2	1	-1	2	2	-3
7	2	1	3	2	-3	-3	5
2	1	0	2	-3	5	11	-18

$$\gcd(41, 25) = 41(11) + 25(-18).$$
$$1 = 41(11) + 25(-18)$$

Thus,

$x = -18\ mod\ 41$
$y = 11\ mod\ 25$

(iv) Suggested solution:

$$18x = 11 \; mod \; 19$$
$$x = \frac{11}{18} \; mod \; 19$$
$$x = 11 \; (18)^{-1} \; mod \; 19$$
$$x = (11)(-1) mod \; 19$$
$$x = (11)(18) mod \; 19 = 198 \; mod \; 19 = 8$$

The verification is not mandatory.
$Verify$:
$$18(8) = 11 \; mod \; 19$$
$$144 = 11 \; mod \; 19$$
$$11 = 11$$

Question 6 (2 marks)

What is Discrete Logarithm problem? Show an example of a signature scheme that relies on the security of discrete logarithm problem.

Suggested answer:

The discrete logarithm problem refers to rules and operations related to mathematical entities called groups. It is defined as follows: given an element g in a group G of order t, and another element y of G, the problem is to find x < p, such that $y = g^x \bmod p$. Like the factoring problem, the discrete logarithm problem is believed to be difficult and also to be the hard direction of a one-way function.

ElGamal Digital Signature

Key generation:

- The key generation algorithm of ElGamal digital signature system is the same as the one employed by the ElGamal asymmetric encryption system.
- For every user, it generates a public ElGamal verification key (*p, g, y*) and a corresponding private ElGamal signing key *x*.
- All users may be using the same *p* and *g*.

Message signing:

- Select a number *k* from Z_p^* such that *gcd(k, p-1)=1*.
- Compute the first element of the signature $r = g^k \; mod \; p$.
- Hash the message *m*, and the result *h(m)* is used to compute the second element of the signature $s = k^{-1} \; (h(m) - xr) \; mod \; (p-1)$

Signature verification:

- Verify that

- $1 \leq r \leq p-1$
- $g^{h(m)} \bmod p = y^r r^s \bmod p$

The signature is valid only if both the verification checks are positive.

Question 7 (2 marks)

Describe how encryption and decryption works for a cryptosystem built from a Feistel network.

Suggested answer:

Encryption:

- To encrypt a message, the message is broken down into two equal halfs of 32-bits, a left-half (L_0), and a right-half (R_0).
- The messages L_0 and R_0 are passed through multiple rounds of processes, and at each round the process is as follow:

$$L_{i+1} = R_i$$
$$R_{i+1} = L_i \oplus f(R_i, K_i)$$

where
- L_i is the left half of the current round,
- R_i is the right half of the current round, and
- K_i is the key of the current round.

Decryption:

- To decrypt a ciphertext, similarly, the ciphertext is broken down into to equal halfs of 32-bits, a left-half and a right-hafl and passed through multiple rounds of processes as follows:

$$R_i = L_{i+1}$$
$$L_i = R_{i+1} \oplus f(R_i, K_i) = R_{i+1} \oplus f(L_{i+1}, K_i)$$

where
- L_i is the left half of the current round,
- R_i is the right half of the current round, and
- K_i is the key of the current round.

Question 8 (2 marks)

(i) Consider the RSA algorithm where $p = 11, q = 13,$ and $e = 11$. You receive the ciphertext c = 106. Find the plaintext or message m.

(ii) Adam and Barbie share the same modulus n for RSA to generate their encryption key e_A and e_B. Charlie sends them (Adam and Barbie) the same message m encrypted with e_A and e_B respectively. The resulting ciphertexts are c_A and c_B. Eve intercepts both c_A and c_B. Show how Eve can use the *common modulus attack* to compute the plaintext or the message m sent by Charlie?

Suggested answer:

(i)

Key generation:

- Given p = 11 and q = 13, compute the modulus n = p x q = 11 x 13 = 143.
- Compute $\phi(n) = (p-1)(q-1) = 10 \times 12 = 120$.
- Since e is given as 11, d can be determined by finding the inverse multiplicative of e mod ϕ(n) using the extended Euclidean Algorithm as follow:

n1	n2	r	q	a1	b1	a2	b2
120	11	10	10	1	0	0	1
11	10	1	1	0	1	1	-10
10	1	0	10	1	-10	-1	11

Thus d = 11.

The plaintext m can then be obtained as follow:

$m = c^d \ mod \ n$

$m = 106^{11} \ mod \ 143$

$m = 7 \ mod \ 143$

$m = 7.$

(ii)

Eve knows the ciphertext $c_A \equiv m^{e_A} \ mod \ n$ and $c_B \equiv m^{e_B} \ mod \ n$. Eve also knows that the $\gcd(e_A, e_B) = 1$. Thus Eve can compute the inverse multiplicative of e_A and e_B using extended Euclidean Algorithm to get $(e_A)(a) + (e_B)(b) = 1$.

Eve then computes $(c_A)^a \cdot (c_B)^b \ mod \ n$, which she can obtain the message m as follow:

$= (m^{e_A})^a \cdot (m^{e_B})^b \ mod \ n$

$= (m^{e_A \cdot a}) \cdot (m^{e_B \cdot b}) \ mod \ n$

$= m^{(e_A)(a)+(e_B)(b)} \ mod \ n$

$= m \ mod \ n$

$= m$

END OF TEST