3(a) 26!. Since x has a distinct mapping to y and y has to map to x, the first mapping has 26 possibilities, the second has 25, the third has 24, etc. Thus, the total number of mapping is the factorial of 26, i.e., 26!.

3(b) The number of possible plaintext letter is limited, say, 26, one can encrypt each letter of the plaintext to get ciphertext, so we have 26 plaintext-ciphertext pair. Any incoming ciphertext can be mapped directly to corresponding plaintext by looking up the mapping table.

4(a)

FUNCTION INVERSE(a, n):

If GCD(a, n) == 0:

Return ‘not exist!’

If n is a prime number:

Return a^(n-1)

Else:

Return a^(phi(n))

4(b)

i) Since GCD(12, 39) != 1, 12^-1 mod 39 does not exist.

ii) Since 12986\*8905 + 46799\*(-2471) = 1, 12986^-1 mod 46799 = 8905

iii) Since 17\*12 + 29\*(-7) = 1, 17^-1 mod 29 = 12

iv) 12^-1 mod 17 = 10

v) Since 31 is a prime number and is relatively prime to 12, we have 12^30 mod 31 = 1.

Now we have 12^29 mod 31 = 13, so 13 is the inverse modular of 31.

vi) Since 31 is a prime number and is relatively prime to 10, we have 10^30 mod 31 = 1.

Now we have 10^29 mod 31 = 28, so 28 is the inverse modular of 28.

5(a) A hash function, by itself, does not provide message authentication. A secret key must be used in some fashion with the hash function to produce authentication. A MAC, by definition, uses a secret key to calculate a code used for authentication.

5(b)

i) s^e =? h(m).

ii) The consequence of failure of second preimage resistance is the computation to find another x’ such that h(x’) = h(x) is feasible. The security of this system is not guaranteed, in particular, the signature can be forged by others easily, since we can find another message m’ such that h(m) = h(m’).

5(c) One-way property: It is computationally feasible to compute h(x) given x, but infeasible to reverse x given h(x).

Second preimage resistance: Given h(x), it is computationally infeasible to find another x’, such that h(x) = h(x’).

Collision resistance: It is computationally infeasible to find a pair of x and x’, such that h(x) = h(x’).

6(a) ① , [1, 0, 1]; ② , [1, 1, 1]; ③ , [1, 1, 0]; ④ , [0, 1, 1].

6(b)

6(c)

7(a)

, ; ,

7(b) Using the same k can compromise the private key because of multiplicative property.

7(c) One can forge a signature using this scheme.

8.

9. (a) random positive integer; (b) ; (c) ; (d) .

10(a) cipher block chaining

10(b) i) initial vector; ii) symmetric key; iii) j-th ciphertext block; iv) j-th plaintext block; v) encrypted message of x with the key of y.

10(c) i) ; .

11(a) timestamp that avoids replay attack.

11(b)

When a sender’s clock is ahead of the intended recipient’s clock, an opponent can intercept a message from the sender and replay it later when the timestamp in the message becomes current at the recipient’s site. This replay could cause unexpected results.

An unintentionally post-dated message (message with a clock time that is in the future with respect to the recipient’s clock) that requests a key is sent by a client. An adversary blocks this request message from reaching the KDC. The client gets no response and thinks that an omission or performance failure has occurred. Later, when the client is off-line, the adversary replays the suppressed message from the same workstation (with the same network address) and establishes a secure connection in the client’s name.

An unintentionally post-dated message that requests a stock purchase could be suppressed and replayed later, resulting in a stock purchase when the stock price had already changed significantly.