Question1:

Answer: 13104584 + 3334 mod 26 = 18

CRYPTOGRAPHYISINTERESTING - plaintext

UJQHLGYJSHZQAKAFLWJWKLAFY - cipertext

Question2:

a): letter sequence K (based on X): RPRCTOGT

b): Ciphertext: TPWTORFGHAKWKQHQODOGYDHQBV

The square is:

R P C T O

G A B D E

F H I K L

M N Q S U

V W X Y Z

CR YP TO GR AP HY IS IN TE RE ST IN GX

(substitute “x” on the last pair)

TP WT OR FG HA KW KQ HQ OD OG YD HQ BV

Question 3:

1. F(x, key) = x XOR key

We could use x times brutal attack to reverse this encryption

2. We assume this encryption is a RSA encryption

denote y as the ciphered text

x = y ^ k3 (mod k2)

k3 is k1's modular inverse (mod k2)

Since we could choose a large prime number as k2 and the time complexity on finding the factors of k2 could outnumber it of x times brutal attach to reverse the first algorithm. The second algorithm is better to be used as encryption algorithm.

Question 4:

Answer: 2^56/(10^10\*2) ≈ 41.68 days

Question 5:

Answer: The advantage of EDE over EEE lies principally in hardware implementations. A EEE DES structure cannot preserve compatibility with DES; a hardware circuit that implemented 3DES (with EDE) could also be used to do DES as well (by, say, making all three sub-keys the same). Recalling that originally, only hardware implementations complied with the standard, a chip that implements EDE is "backwards compatible" with single DES, whereas a chip that implements EEE is a completely different cipher.

if we select the first two sub-keys to be the same weak key, the second encrypt with the weak key would exactly undo the first, and the plaintext block will be operated on by the third sub-key (which is the DES operation we really want).

Now, if we had a 3DES EEE implementation with three independent sub-keys, we could support DES (using the weak key trick), 2 key 3DES (EEE), and 3 key 3DES (EEE). However, that wasn't the only situation they had in mind; they also considered the case where someone implemented 2 key 3DES in hardware (which the first and last sub-keys were constrained to be the same). That's one thing EEE mode can't do; we can't use the weak sub-key trick with 2 key 3DES (if we make two of the adjacent sub-keys the same weak key, then all three sub-keys are the same weak key). However, the EDE trick still works.

Also, two keys 3DES using EDE mode could use less key space in the matter of key storage than three keys 3DES using EEE mode.

Question 6:

a).

29\*35 (mod 78) = 1

Hence the modular inverse of 35 (mod 78) is 28.

b).

5\*3485 (mod 5808) = 1

2266^3485 (mod 5963) = 23

Hence the plaintext is 23.

Question 7:

a):

A "normal", brute-force attack on a cryptographic hashing algorithm HH should have a complexity of about 2n for a hash algorithm with an output length of n bits. That means it takes about 2^(n−1) tries on average to find a colliding message y for a given message x so that H(y)=H(x) while y≠x. However, a birthday attack (e.g. both x and y can be selected arbitrarily, but H(x)=H(y) is of course still required) is supposed to be much faster, and take only 2^(n/2) tries to find a collision.

In this case the answer is 2^64 tries.

b):

The weak collision resistance property is sometimes also referred to as second pre-image resistance:

“Given an arbitrary x there exists no x' with x' != x so that h(x) = h(x')”

Strong collision resistance on the other hand is defined as:

“There exist no x and x' with x != x' so that h(x) = h(x')”

It requires a hash value at least twice as long as that required for pre-image resistance, otherwise collisions may be found by a birthday attack.

The obvious difference in their definitions is that for weak collision resistance we assume to be bound to a particular choice of x, whereas in the definition of strong collision resistance we are free to arbitrarily choose our x and x'. As the name implies, it is more difficult to achieve strong collision resistance than weak collision resistance. This is because strong collision resistance implies weak collision resistance, yet, having weak collision resistance does not imply strong collision resistance.

Therefore, strong collision may be harder to break than weak collision.