Mid Term Cryptography

1. Process of encryption and decryption in relation to cryptography

- Encryption is the process of converting plain text to become cipher text using encryption algorithm called cipher and a secret value called key.
- Decryption is the process of reversing back the cipher text to become plain text, given user has the secret key to decrypt it.
- The cryptography principle is if we don't know the secret key, you can't decrypt, nor can you learn any bit of information on the encrypted message; and neither can any attacker.
- This is very important to protect the information secrecy when transmitting and ensure the message confidentiality by transforming the plain text that readable to something that is completely unreadable.

2. The weakness in DES algorithm.

- DES is weak against brute force attack because in 1977 Diffie and Hellman proposed a machine costing an estimated US$20 million which could find a DES key in a single day, because the increase in computing power every single year makes it possible.
- The prediction became reality in 2006 when DES cracker COPACOBANA machine built by the teams of the University of Bochum and Kiel in Germany that cost effective because reduced the time to break DES in less than one day and can be built for approximately $10 000.
- Two chosen input to an S-box can create the same output, which can be exploited if not taken care of. Another one is the purpose of initial and final permutation is not clear, which begs the question of why NSA made the modifications to the cipher in first place.

- DES is weak against differential-linear cryptanalysis that was proposed by Langford and Hellmann in 1994. It combines differential and linear cryptanalysis into a single powerful attack.

3. Interpret the secret message produced from the plaintext using Vigenere Cipher.

- `Plaintext: "Life is full of surprises"`
- `Keyword:   "HEALTH"`

Plaintext	L I F E I S F U L L O F S U R P R I S E S
Keyword	H E A L T H H E A L T H H E A L T H H E A
Ciphertext	S M F P B Z M Y L W H M Z Y R A K P Z I S

4. List the parameters (block size, key size and the number of rounds) for 3 AES versions.

AES-128:

- The length of the input block size is 128-bits.
- Use cipher key or key size with length of 128-bits.
- The number of rounds to be performed during the execution is 10 rounds.

AES-192:

- The length of the input block size is 192-bits.
- Use cipher key or key size with length of 192-bits.
- The number of rounds to be performed during the execution is 12 rounds.

AES-256:

- The length of the input block size is 256-bits.
- Use cipher key or key size with length of 256-bits.
- The number of rounds to be performed during the execution is 14 rounds.

5. Compare the substitution in DES and AES.

Data Encryption Standard	Advanced Encryption Standard
The data block is divided into two halves, left and right before the main algorithm starts.	The entire data block is processed as a single matrix.
DES works based on Feistel Cipher structure.	AES works on substitution and permutation principle.
Plaintext size is 64-bits.	Plaintext can be 128, 192 and 256-bits.

6. Decrypt the message GZD KNK YDX MFW JXA if it was encrypted using a shift cipher with shift of 5.

- `Ciphertext: G Z D K N K Y D X M F W J X A`
- `Plaintext:  B U Y F I F T Y S H A R E S V`