**Cipher text only attack:**

Attacker Must Know for each atk type:

* In cipher text only attack, attacker used to access the as much as encrypted messages.
* At the same time attakcer doesnt have any ider regarding the secret key and plaintext also.
* After collecting the encrypted messages, attacker implement different trails to guess the secret key, which is known as encrypted key.
* When attacker discover the encrypted key then he break all the other messages which have been encrypted by this key.

**Known-plaintext attack:**

* The crypto attack that used to access the both plaintext and ciphertext is known as Known-plain text.
* When attacker have both plain text and its corresponding plain text that will help to find the algorithm or to develop an algorithm regarding the encryption process.
* After developing the algorithm that would help to attacker to break the all other messages.

**Chosen-Plaintext attack:**

* The chosen-plaintext attack allows to collect random number of plaintexts to obtain the corresponding ciphertexts.
* After obtaining the ciphertexts, that helps the attacker to acquire the secret key or alternatively to create an algorithm.
* That algorithm or secret key will help to break the encrypted messages.

**Design Principles for Protection Mechanisms**

* Least priviledge (operate w/ only necessary privileges)
* Complete mediation (access to objects are checked efficiently)
* Open design (don’t depend on secrecy of design)
* Separation of priviledge (req. 2 keys to access o2bj.)
* Fail-safe defaults
* Least common mechanism (minimize common mechanism use)
* Psychological acceptability (UI is easy to use)

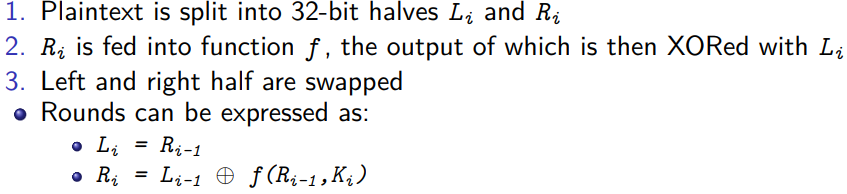
**Access Control Policies**

* Discretionary access ctrl. (DAC – ctrl access based on ID of requestor)
* Mandatory Access Ctrl. (MAC – compare security level w/ clearance)
* Role Based AC – (RBAC – user has roles and sys. Determines role access)
* Attribute based (ABAC – ctrl based on user attributes)

**Security models**

* BLP: read down, write up (confidentiality)
  + Strong tranquility – security labels never chg.
  + Weak tranq. – sec. label chg. If policy isn’t violated
* Biba no read down, no write up (integrity)

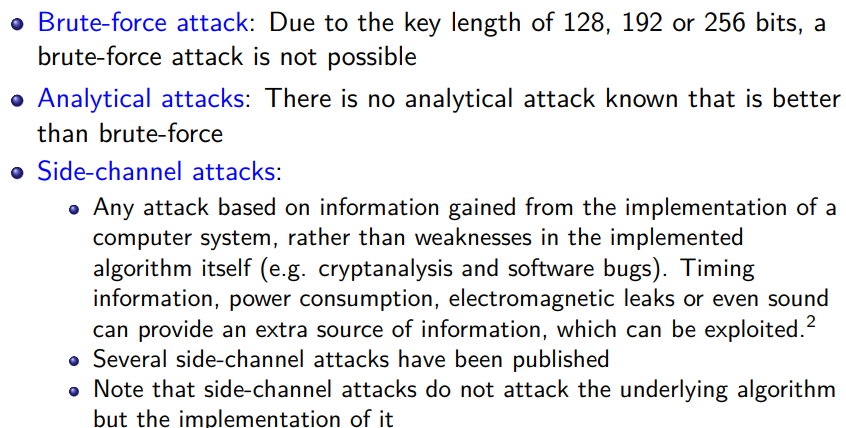
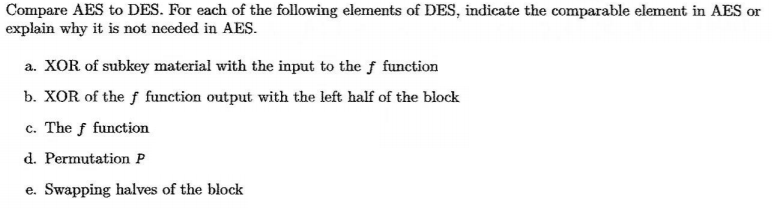
**DES (3DES is DES with 3 diff keys done 3 times)**

* 

Then s-box sub at (Ri = …)

Then (Li,Ri) then 16 permutations

**AES**

* 
* 

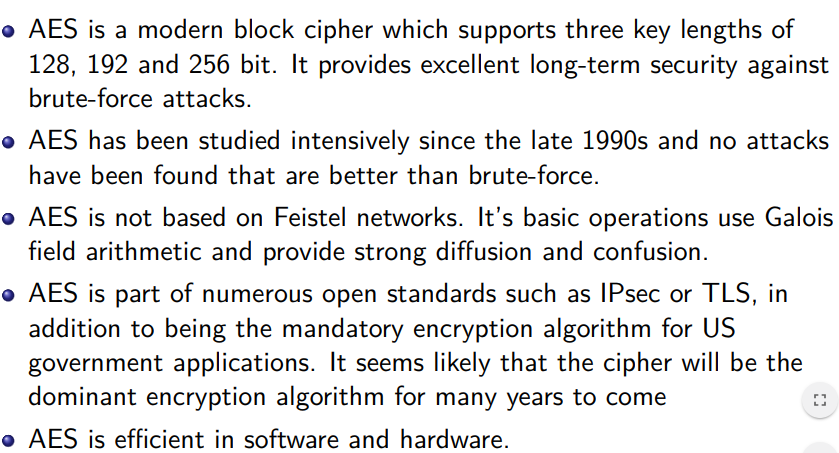
Key addition

des is feistel struct and AES doesn’t

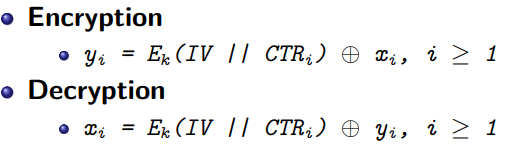
byte sub.

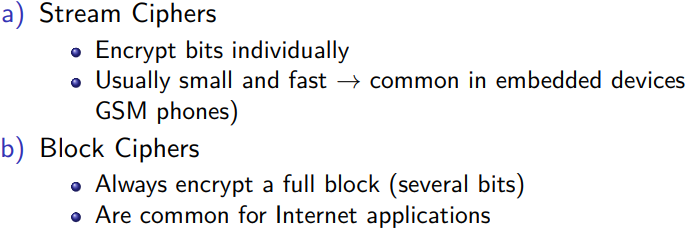
Shift rows sublayer & mix col. Sublayer

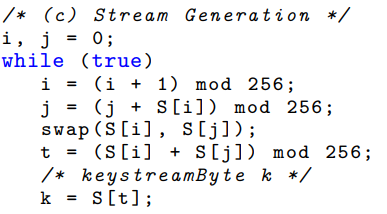
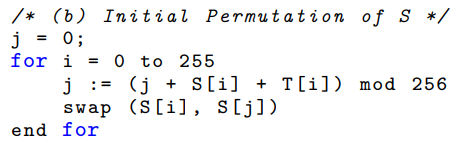
AES has no swappable halves; no feistel struct

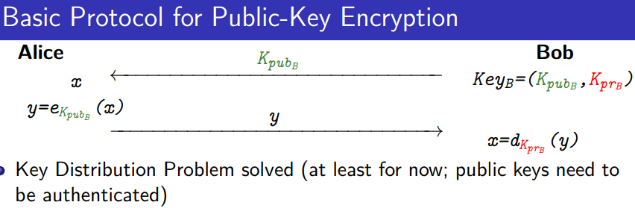
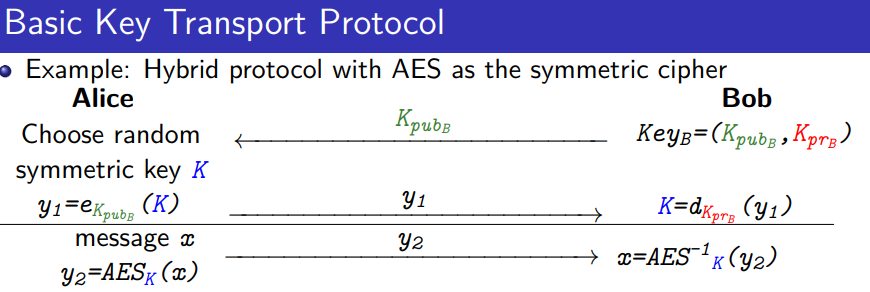
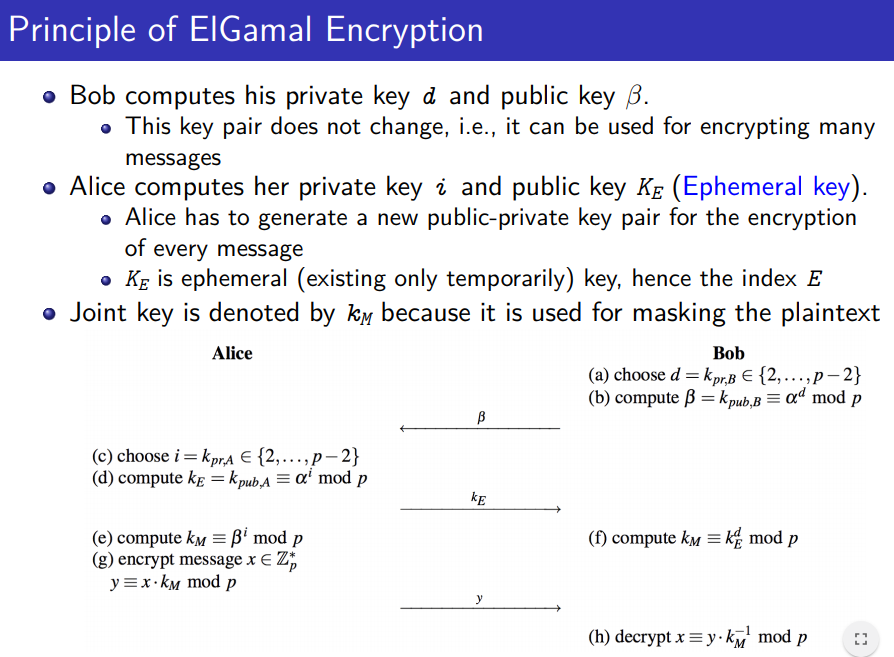
* 

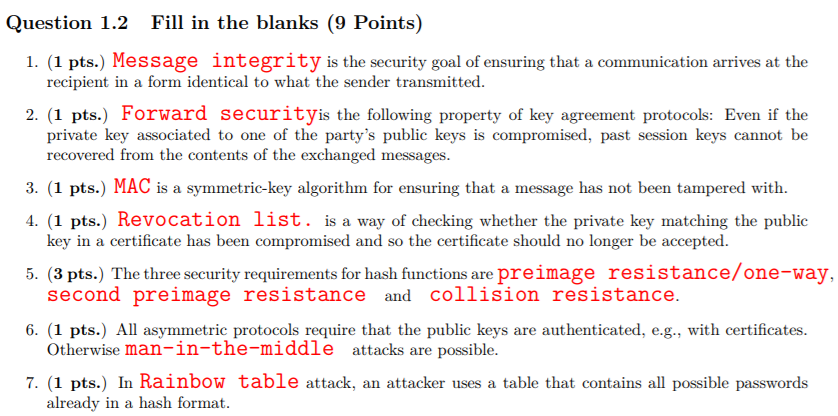
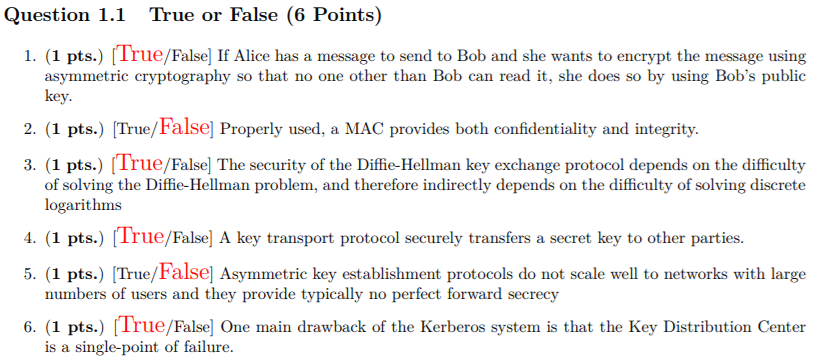
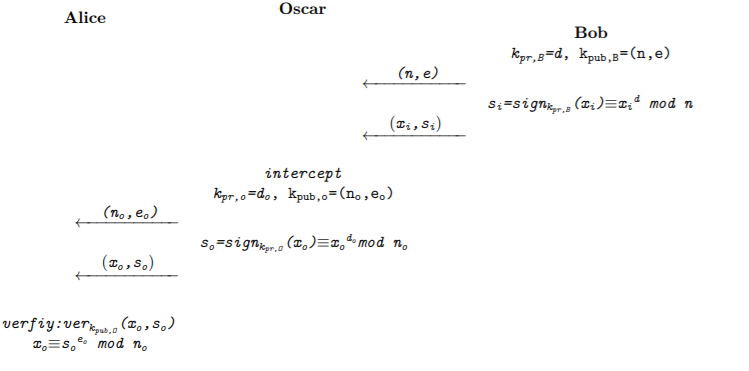
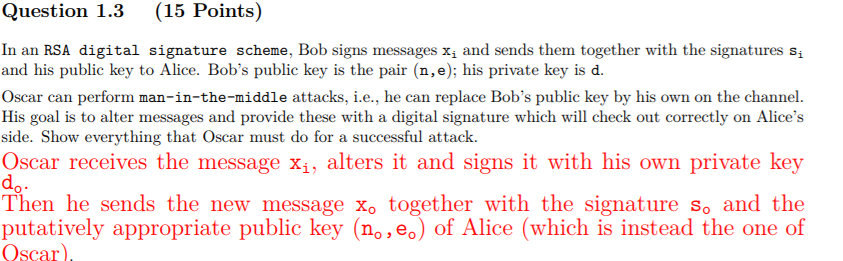
CTR mode req: n bits= Capacity/block size



* 
* **RC4:**



* ****
* ****
* 

****

