**-Mention the Five modes of operation of Block Cipher?**

1. Electronic Codebook Book (ECB)
2. Cipher Block Chaining (CBC)
3. Cipher FeedBack (CFB)
4. Output FeedBack (OFB)
5. Counter (CTR)

**-Sketch the Output Feed Back Mode diagram and write the necessary equations for encryption and decryption?**

<u>Encryption</u>

$O_i = E_K(O_{i-1})$

$C_i = P_i$ XOR $O_i$

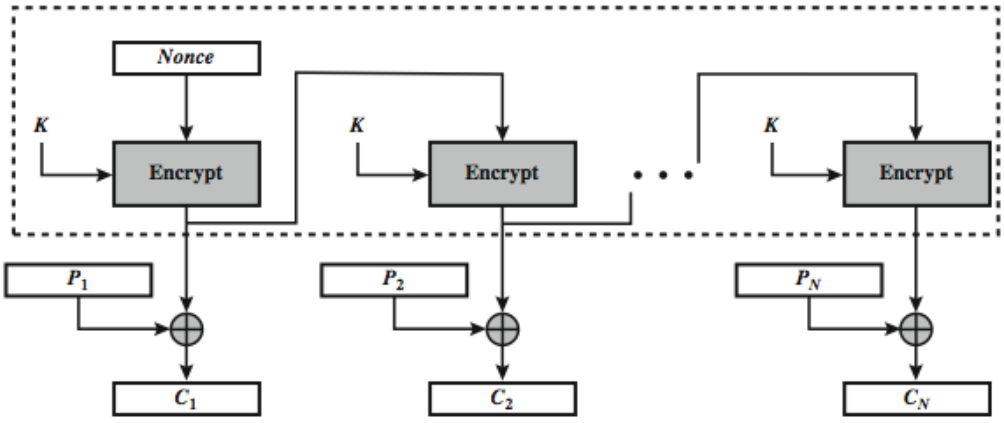
$O_{-1} = IV$

<u>Decryption</u>

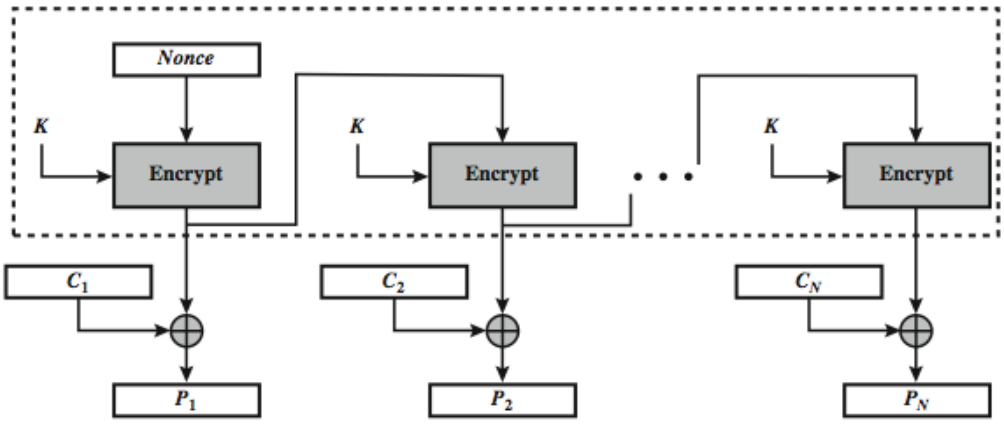
$O_i = E_K(O_{i-1})$

$P_i = C_i$ XOR $O_i$

$O_{-1} = IV$




(a) Encryption




(b) Decryption

**-Compare between OFB Advantages and Disadvantages?**

| Advantages: | Disadvantages: |
| --- | --- |
| - Bit errors in transmission do not propagate | - More vulnerable to a message stream modification attack<br>- Needs an IV which is unique for each use |

**-Write Equation of Diffie-Hellman Algorithm and solve the following question?**

Global Public Elements

q: prime number

a: a < q and primitive root of q

User A Key Generation

Select private XA , XA < q

Calculate public YA, $YA = a^{YA} \bmod q$

User B Key Generation

Select private XB , XB < q

Calculate public YB, $YB = a^{XB} \bmod q$

Calculation of Secret Key by User A

$K = (YB)^{XA} \bmod q$

Calculation of Secret Key by User B

$K = (YA)^{XB} \bmod q$

**-What is the shared Secret Key?**

$K = (YB)^{XA} \bmod q = (YA)^{XB} \bmod q$

Used for subsequent encryption of messages between A and B

**-what are the characteristics needed in secure hash function?**

| Requirement | Description |
|---|---|
| Variable input size | H can be applied to a block of data of any size. |
| Fixed output size | H produces a fixed-length output. |
| Efficiency | $H(x)$ is relatively easy to compute for any given $x$, making both hardware and software implementations practical. |
| Preimage resistant (one-way property) | For any given hash value $h$, it is computationally infeasible to find $y$ such that $H(y) = h$. |
| Second preimage resistant (weak collision resistant) | For any given block $x$, it is computationally infeasible to find $y \neq x$ with $H(y) = H(x)$. |
| Collision resistant (strong collision resistant) | It is computationally infeasible to find any pair $(x, y)$ such that $H(x) = H(y)$. |
| Pseudorandomness | Output of H meets standard tests for pseudorandomness. |

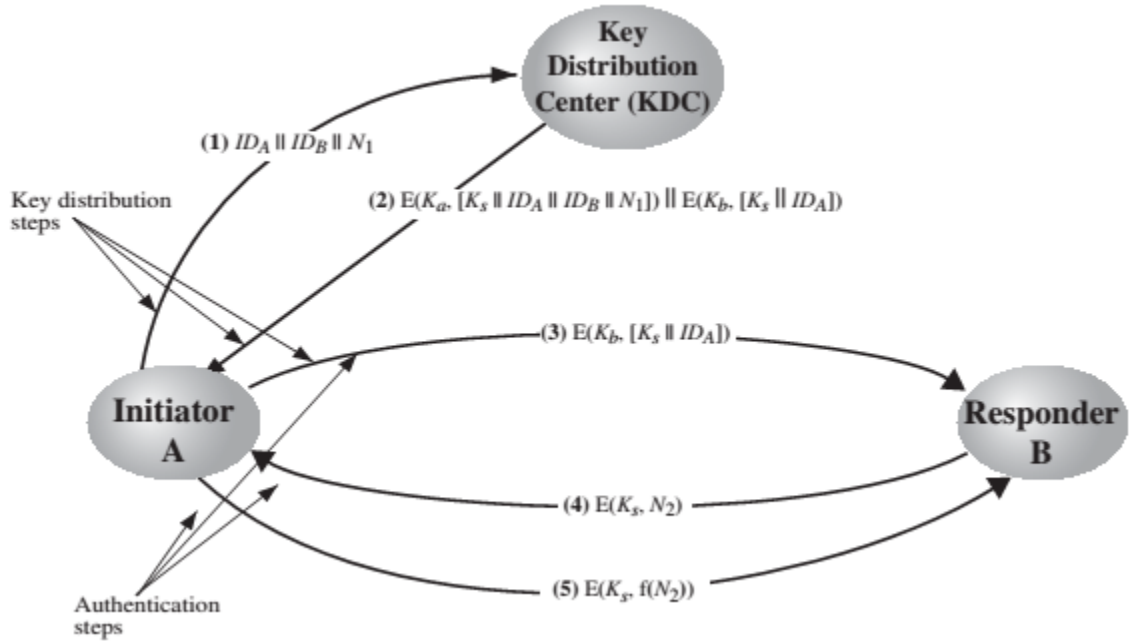
**-Mention 3 objective of the HMAC Design?**

• To use, without modifications, available hash functions. In particular, to use hash functions that perform well in software and for which code is freely and widely available.
• To allow for easy replaceability of the embedded hash function in case faster or more secure hash functions are found or required.
• To preserve the original performance of the hash function without incurring a significant degradation.
• To use and handle keys in a simple way.
• To have a well understood cryptographic analysis of the strength of the authentication mechanism based on reasonable assumptions about the embedded hash function.

**-what types of attack are addressed by message authentication?**

1. Disclosure: Release of message contents to any person or process not possessing the appropriate cryptographic key.
2. Traffic analysis: Discovery of the pattern of traffic between parties. In a connection-oriented application, the frequency and duration of connections could be determined. In either a connection-oriented or connectionless environment, the number and length of messages between parties could be determined.
3. Masquerade: Insertion of messages into the network from a fraudulent source. This includes the creation of messages by an opponent that are purported to come from an authorized entity. Also included are fraudulent acknowledgments of message receipt or nonreceipt by someone other than the message recipient.
4. Content modification: Changes to the contents of a message, including insertion, deletion, transposition, and modification.
5. Sequence modification: Any modification to a sequence of messages between parties, including insertion, deletion, and reordering.
6. Timing modification: Delay or replay of messages. In a connection-oriented application, an entire session or sequence of messages could be a replay of some previous valid session, or individual messages in the sequence could be delayed or replayed. In a connectionless application, an individual message (e.g., datagram) could be delayed or replayed.
7. Source repudiation: Denial of transmission of message by source.
8. Destination repudiation: Denial of receipt of message by destination.

**-Draw Needham Schroeder Protocol (KDC) , write equation and specify all the details of it ?**




1. A requests from the KDC a session key to protect a logical connection to B. The message includes the identity of A and B and a unique *nonce N1.*

2. The KDC responds with a message encrypted using *Ka* that includes a one-time session key *K*s to be used for the session, the original request message to enable A to match response with appropriate request, and info for B

3. A stores the session key for use in the upcoming session and forwards to B the information from the KDC for B, namely, E(*Kb, [Ks || IDA])*. Because this information is encrypted with Kb, it is protected from eavesdropping.

At this point, a session key has been securely delivered to A and B, and they may begin their protected exchange. Two additional steps are desirable:

4. Using the new session key for encryption B sends a nonce *N2 to A.*

5. Also using Ks, A responds with f(N2), where f is a function that performs some transformation on N2 (eg. adding one). These steps assure B that the original message it received (step 3) was not a replay. Note that the actual key distribution involves only steps 1 through 3 but that steps 4 and 5, as well as 3, perform an authentication function.

**- If we tried to use the Needham Schroeder Protocol in the E-mail Application what the modifications to be done on it?**

Remove steps 4 & 5 as B is offline

**-Identify Classes of intruders?**

• Masquerader: An individual who is not authorized to use the computer (outsider)

• Misfeasor: A legitimate user who accesses unauthorized data, programs, or resources (insider)

• Clandestine user: An individual who seizes supervisory control of the system and uses this control to evade auditing and access controls or to suppress audit collection (either)

**-What the common two technique to protect password file?**

• Unix uses multiple DES (variant with salt)

• More recent systems use crypto hash function

**-in intruder detection, what is the difference between statistical anomaly and rule based detection?**

• statistical anomaly detection

- attempts to define normal/expected behavior
- threshold
- profile based

• rule-based detection

- attempts to define proper behavior
- anomaly
- penetration identification

**-what is HoneyPot?**

• decoy systems to lure attackers

- away from accessing critical systems
- to collect information of their activities
- to encourage attacker to stay on system so administrator can respond

• are filled with fabricated information

• instrumented to collect detailed information on attackers activities

• single or multiple networked systems

**-What is a salt in UNIX Password management and why is it used?**

• It prevents duplicate passwords from being visible in the password file. Even if two users choose the same password, those passwords will be assigned at different times. Hence, the "extended" passwords of the two users will differ.

• It effectively increases the length of the password without requiring the user to remember two additional characters. Hence, the number of possible passwords is increased by a factor of 4096, increasing the difficulty of guessing a password.

• It prevents the use of a hardware implementation of DES, which would ease the difficulty of a brute-force guessing attack.

**-List 4 techniques to avoid guessable password?**

• User education

• Computer-generated passwords

• Reactive password checking

• Proactive password checking

**-list and describe the 4 phases of operation of virus and worms?**

• Dormant phase: The virus is idle. The virus will eventually be activated by some event, such as a date, the presence of another program or file, or the capacity of the disk exceeding some limit. Not all viruses have this stage.

• Propagation phase: The virus places an identical copy of itself into other programs or into certain system areas on the disk. Each infected program will now contain a clone of the virus, which will itself enter a propagation phase.

• Triggering phase: The virus is activated to perform the function for which it was intended. As with the dormant phase, the triggering phase can be caused by a variety of system events, including a count of the number of times that this copy of the virus has made copies of itself.

• Execution phase: The function is performed, which may be harmless, e.g. a message on the screen, or damaging, e.g. the destruction of programs and data files

**-describe how does the worm propagate?**

Searches for other systems, connects to it, copies self to it and runs.

**-what is the disadvantage of the one pad time cryptosystem?**

• There is the practical problem of making large quantities of random keys. Any heavily used system might require millions of random characters on a regular basis. Supplying truly random characters in this volume is a significant task.
• Even more daunting is the problem of key distribution and protection. For every message to be sent, a key of equal length is needed by both sender and receiver. Thus, a mammoth key distribution problem exists.

**-Draw Authority Key Distribution mechanism and illustrate all the equation needed?**

**-Draw Certificate Key Distribution mechanism and illustrate all the equation needed?**

-**If RSA Algorithm were used and Bob and Alice where exchanging message, Bob leaks his Private key , and as a solution he decide to generate a new public and private key ?**

**-Is that safe?**

**-Illustrate your answer?**

**-Explain the Double DES and Triple DES and write the needed Equation for them? Draw the block diagram of both?**

**-Why Double Des with two keys each one with size of 56 bits is less secure than Des with one Key with size of 112 bits?**

**-Compute the GCD of the Two Following Polynomial?**

x4+x3+x and x2+1 over GF(2)

b. 2x3+x2+2 and x2+x+1 over GF(3)

**-Compute the Multiplicative inverse of the following F(x) and G(x) in module GF(2^8)**

x5+x4+x2+1 in GF (28) with m(x)= x8+x4+x3+x+1