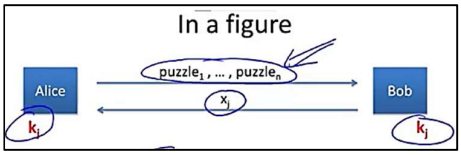
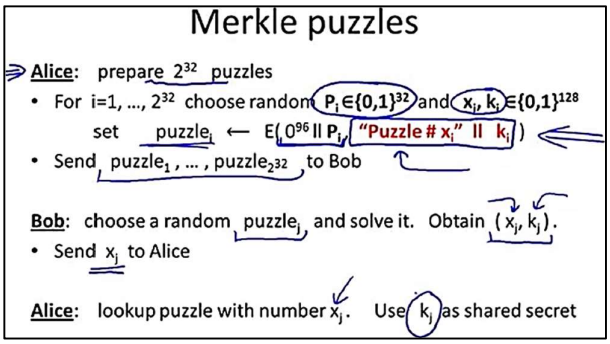
Time: 60 minutes. **Max Points**: 60.

Q1. Explain how a sender (Alice) prepares a Merkle Puzzle to establish a shared key with a second party (Bob). Your answer should list each step that both Alice and Bob perform in this exchange.

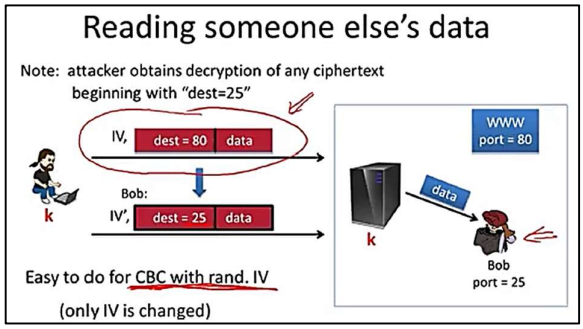
Marks should be awarded for explaining the exchange and how each party drives the shared key. Individual details of constructions of the puzzle should get partial marks only.

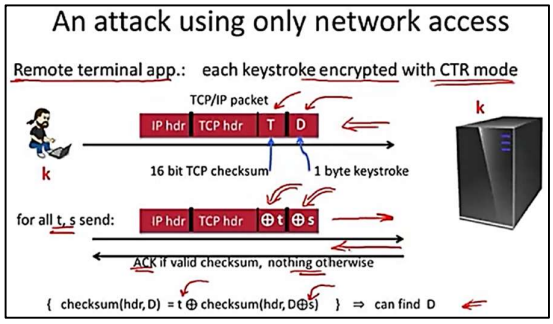




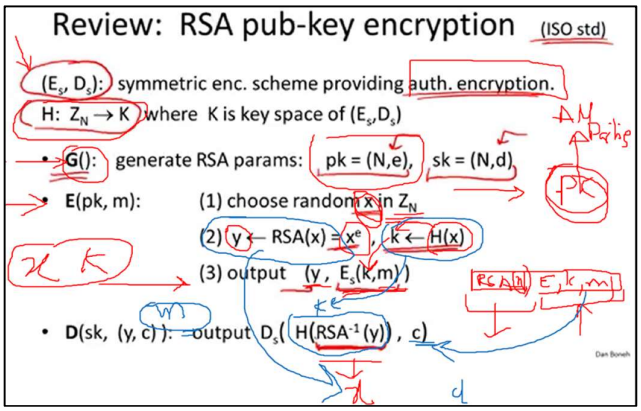
Q2. Illustrate a scenario where an attacker can launch a Chosen Ciphertext Attack (CCA) to compromise encryption without using any brute force methods.

Any one of the follow now scenario covered as part of the syllabus. Marks award to answer explaining the scenario and not explaining the math involved to retrieve the data. Explanation of CCA is not required in this question; rather it is implicit and reflected in the choice of their scenarios.





Q3. What is the role of Asymmetric encryption in secure communication? Show exchanges necessary for secure use of RSA encryption between two parties. Each step needs a brief explanation.



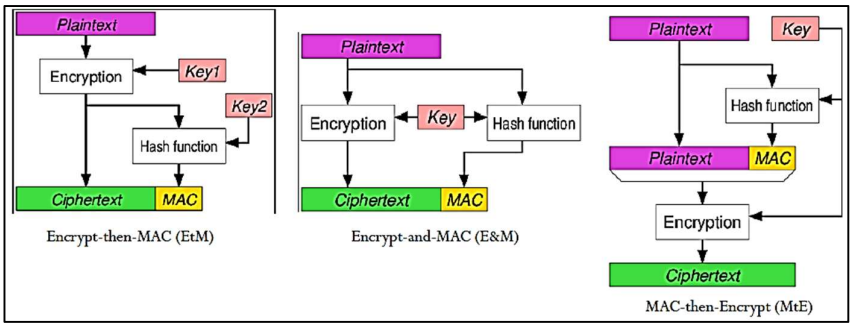
Part # 1: Asymmetric encryption (also known as public key encryption) is used for:

i) Encryption. Messages sent using public key, which is available to everybody. And decryption is done by the receiver using his/her private key (not disclosed to anybody).

ii) Authentication of sender and non-repudiation of messages. Private key can be used to sign messages as it unique identified the person. Anybody can verify it using sender's public key.

Part # 2: The answer should explain both encrypt and decryption step without any omissions.

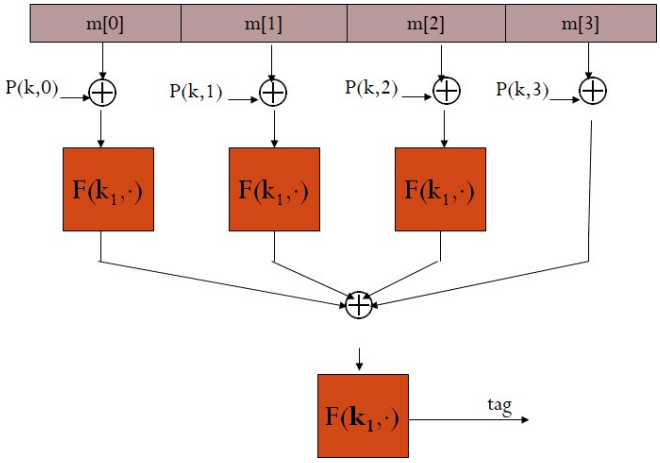
Q4. Explain a mechanism, in steps, to send an encrypted message that prevents an adversary to launch a Chosen Ciphertext Attack.



This question related to authenticated encryption, which ensure avoiding scenario you, explained in Q2 above.

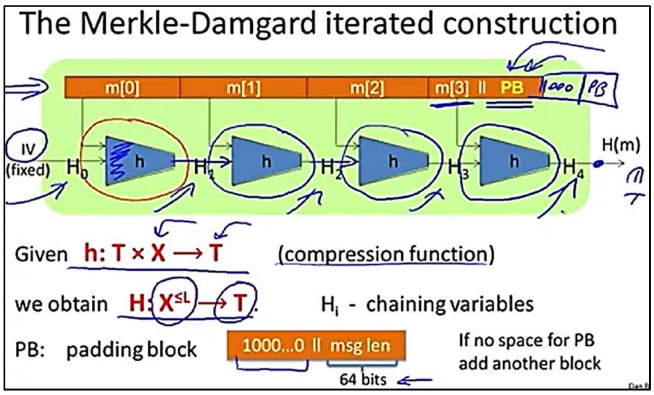
Explain each steps OR
Make a diagram (any one of the three shown here) with short comments explain each step.

Q5. Design a parallel MAC which can be executed using multiple threads. Further, this MAC should also incremental so that for any single block update we do not have to re-compute the whole MAC again.



OR

What is a compression function in the context of MACs? Give a label diagram explaining the Merkle-Damgard Construction of a MAC. Write short labels to explain key concepts.



Part # 1: Compress function is block cipher (also called Davis Meyer compression function) to provide collision resistant output for short messages. It used in iterative way while constructing a MAC (in Merkle-Damgard paradigm) from variable large size message.

Part # 2: See diagram from lecture slides.

Q6. The following is a digital (X.509) certificate:

a. Who issues the certificate? (1)
   Symantec Corporation / Symantec Trust Network
b. Who is the owner of the certificate? (1)
   National Science Foundation
c. Who generated the signature on this certificate and how can this signature be verified? (4)
   Symantemantic (issuer) sign this certificate and receiver will verify it when the owner will send it to her. Root certificates or using chain verifications.
d. The public key contained in this certificate is based on the RSA algorithm. Using the RSA algorithm, to encrypt a message M, we calculate $\mathbf{M^e \bmod n}$. What is the value of e and n in this public key? If a number is too large, you only need to write down its first four bytes. (4)
   e=65537 n=00cafb…6243fd

----------(x)----------