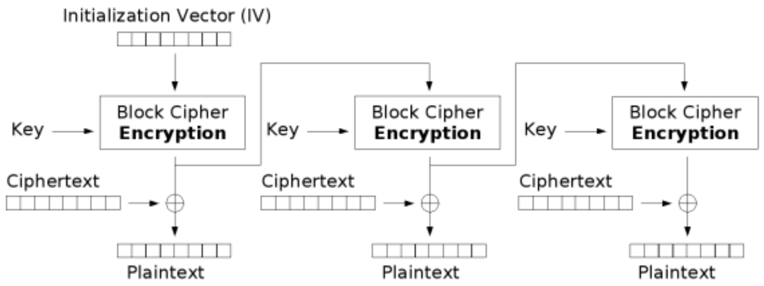
1. Which takes longer to complete, a collision attack or a pre-image attack? Why?
2. In AES, what is the irreducible polynomial?
3. What provides non-repudiation?
4. Does symmetric encryption guarantee message integrity? Why or Why not?
5. Does keeping a system's design and implementation make it more secure? Hint: Kerchoff's principle
6. Which encryption modes require padding?
7. What does Alice need to send Bob in order for him to be sure that the message came from Alice, and was unaltered?
8. Why can Diffie-Hellman be used as a public key exchange?
9. What key does Alice use to to encrypt a message to Bob using public key cryptography?
10. What takes longer, RSA encryption or RSA digital signature? Why?
11. Whose public key is stored in a certificate?
12. What is a relying party?
13. What general hash equation using some hash function H and some key K, is used for the message extension attack, and which is used to thwart the message extension attack?
14. Think about the image below (this exact image will be on the test), and study your homework 2 to think about what attacks could be used, and the possible outcomes.



Output Feedback (OFB) mode decryption

15. How does a certificate hierarchy work? What has to happen if an intermediary certificate is invalidated or revoked?

16. What is the structure of the message performed in the message extension attack? **M1** = Original message, **M2** = attackers message, **P** = padding, **L1** = length of

original message, **L2=** length of total attack, **H1**= hmac of original message, **H2**= hmac of attackers message

17. What is used for encryption? Think of any that we have talked about in class (regardless of how briefly)
18. Which of the following crypto algorithms are still secure? What makes them secure?
    a. AES
    b. DES
    c. MD5
    d. SHA-1
    e. SHA-2
    f. SHA-3
    g. RSA
    h. MAC
    i. HMAC
19. What is a side channel attack?
20. Think about the SHA-1 Diagram below. What size message would produce a padding of 10? 100? 150?

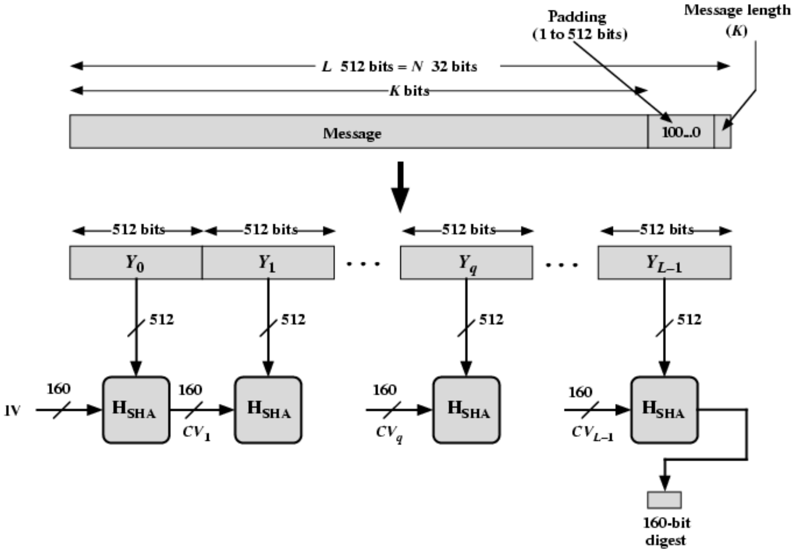


Figure 3.4 Message Digest Generation Using SHA-1

21. How does the Diff-Hellman key exchange work?
22. Create an RSA keypair from p=17, q=11, e=7; and give me the public and private keys.