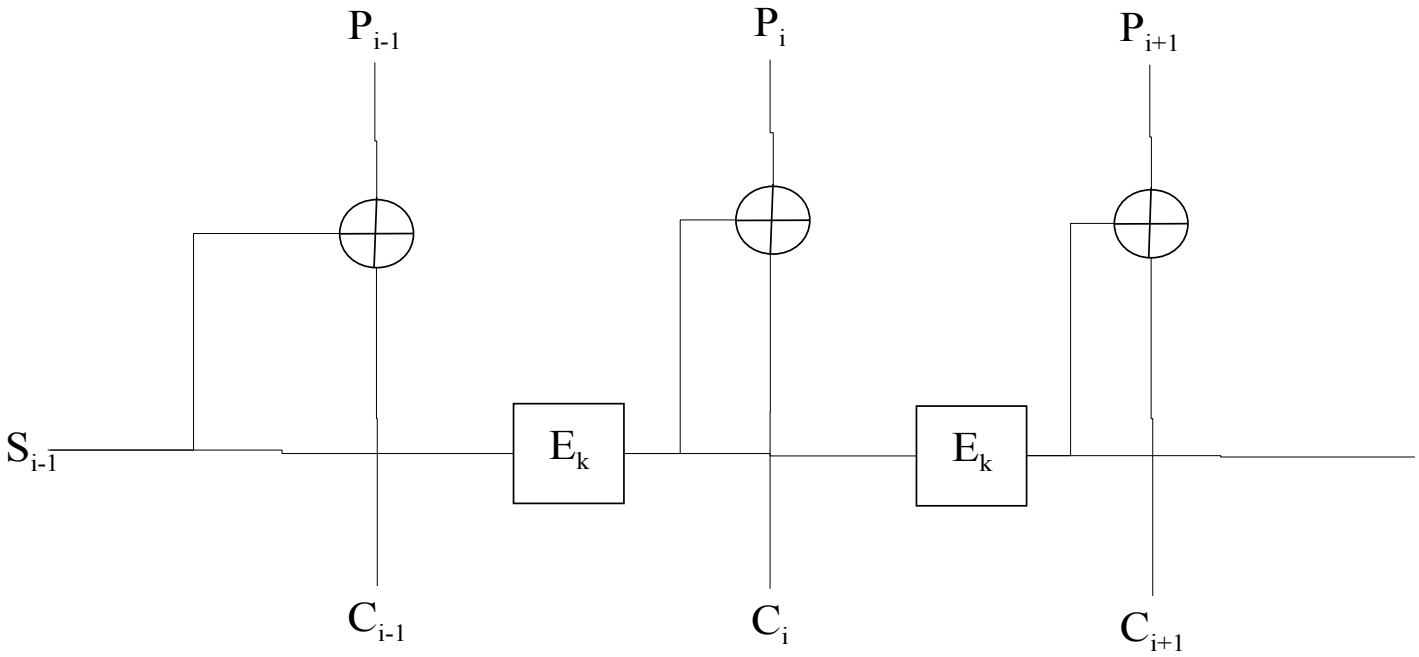
Net ID:

University of Illinois at Urbana-Champaign
Department of Computer Science
Midterm 1 – Answers and Comments
CS461/ECE422 – Computer Security I
Fall 2010
Wednesday, October 6, 2010
Time Limit: 50 minutes

Information Assurance: Midterm 1

Multiple Choice – 3 points each

1. The picture below corresponds to which standard mode that can use block algorithms like AES and DES.



a. Cipher Feedback Mode
b. Cipher Block Chain Mode
c. Electronic Code Book Mode
d. Output Feedback Mode

A lot of people missed this one. The first two options have two stpes, but one step is the client authenticating itself to the server, and the other is the server authenticating itself to the client. The last option only has one authentication element. This leaves C, which uses to factors for authentication: the 6 digit pin (something you know) and information from a secure card (something you have).

2. Which of the following is the best example of multi-factor authentication?
    a. Customer enters password on bank web site and reviews a previously selected picture displayed by the bank web site.
    b. Customer's browser verifies the validity of the bank web site's certificate, and customer enters password on bank web site.
    c. Customer enters a 6 digit pin on the secure card that his bank gave him, and the secure card displays a 12 digit code that the customer enters on the bank web site.
    d. Customer enters a password on the bank web site.

3. You are given a section of cipher text. You know nothing about the encrypting algorithm. You compute the character frequencies in the message. The character frequencies are close to the standard character frequencies you would expect to see in a segment of English text. Based on this information, you believe that the type of encryption algorithm is:
    a. Polyalphabetic
    b. Substitution
    c. Transposition
    d. Product

4. The numbers of steps in a brute force attack on a system that is using DES with two keys to double encrypt the plaintext is:
    a. 2^{56}
    b. 2^{57} - Thanks to the meet-in-the-middle calculation.
    c. 2^{112}
    d. 2^{128}

5. The introduction of a nonce into a key exchange algorithm thwarts which attack?
    a. Replay attack
    b. Key cracking
    c. The man-in-the-middle attack
    d. The meet-in-the-middle attack

6. What is the block size for AES-192 encryption algorithm?
    a. 64
    b. 128
    c. 192
    d. 256

7. Annual Loss Exposure (ALE) is used in quantitative risk risk analysis. What is the similar concept used in qualitative risk analysis?
    a. Threat Priority
    b. Loss Impact
    c. Total Impact
    d. Risk Leverage

8. Which hash algorithm would be most appropriate for generating hash of a software package posted on the main corporate web site? In this scenario customers may be downloading the software package from mirror sites or other locations not directly under the corporation's control.
    a. MD5
    b. HMAC-MD5
    c. CRC
    d. RSA

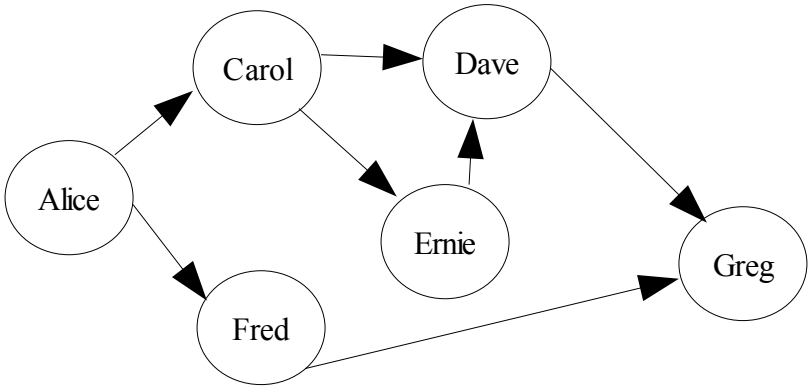
Short answer

9. (12 pts) Consider the list below. Classify each item as an asset, a threat, or a vulnerability.

Item	**Asset, Vulnerability, or Threat?**
Data Servers	*Asset*
Employees write passwords sticky notes and leave them on their monitors	*Vulnerability*
Design for the next generation widget	*Asset*
Tornado	*Threat*
Data center built on a flood plain	*Vulnerability*
Disgruntled employee with knowledge of the organizations computer system structure	*Threat. I also took vulnerability here.*

Net ID:

10. (16 pts) The diagram below shows the web of trust diagram of the certificates that Alice has on her key ring. An arrow from name1 to name2 means that the entity associated with name1 has signed the certificate associated with name2 (e.g., in the diagram below Carol has signed Dave's certificate).



a. To ensure that your signatures are considered trustworthy by others, what is one thing you should ~~be~~ do before signing another person's certificate? (4 pts)

Most people missed this. You should check out the individual. Either by meeting him and checking his ID. Or only signing certificates for people you know and using fingerprint information to verify any certificate you receive from them in the mail.

A lot of people wanted to verify the certificate by checking other signatures on the certificate. This got partial credit. Certainly you should only sign well formed certificates. Though if they were ill-formed, some later user of the certificate should be able to spot that. Since you are signing the certificate, it is quite possible that there are no signatures on the certificate yet anyway.

b. Alice has indicated that she fully trusts Carol and Fred. She marginally trusts Dave and Ernie. How many fully trusted signature chains exist to Greg's certificate? How many marginally trusted signature chains exist to Greg's certificate? What are the paths? (6 pts)

1 fully trusted path: Fred-> Greg
2 marginally trusted paths: Dave->Greg and Ernie->Dave->Greg

Base Certificate
Identity name
Public Key
Expiration Date

Signer Certificate
Signer Identity
Signed Hash

c. The diagram to the side shows the key fields of the base certificate and the signature certificate packet. Assume a certificate uses RSA key pairs. Show the data, equations, and comparisons, you would need to check to verify Carol's signature on Dave's certificate. (6 pts)

Say Carol's public key is (e,n)
SH = the Signed Hash field of Carol's signers certificate for Dave.
H = Hash(Dave's Base Certificate)
$H' = SH^e \bmod n$
Check that H = H'

11. (15 pts, 5 pts each) Consider pen and paper ciphers

a. Decipher the following ciphertext using the rail cipher.

AMSDNNWLOTOEOX

ALMOST DONE NOW X

b. Encrypt "To be or not to be" using a three columnar transposition cipher.

TENTEOOOOXBRTBX

Some people did not add pad characters. These will be needed to decrypt correctly.

Some people wrote the matrix in column major instead of row major order.

c. Decrypt XRAZFE encrypted by Vigenere's algorithm using the key TEST.

ENIGMA

12. (12 pts) Alice and Bob are using the Diffie-Hellman algorithm to generate a common shared key.
    a. What is the equation that Alice will use to compute the number that she will send to Bob?

Alice picks a private value k_A. Alice and Bob have agreed upon a prime p and a relatively prime g.

She sends Bob $K_A = g^{kA} \bmod p$

    b. What is the one major piece of data that Alice and Bob must each keep private when computing the common shared key?

Alice and Bob must keep their private values private. k_A and k_B respectively.

    c. The discovery of an efficient solution for what hard problem will eliminate the strength of the Diffie-Hellman algorithm? Why?

An efficient algorithm for computing discrete logarithm would destroy the strength of the Diffie-Hellman algorithm. Then an observer could take K_A and solve for k_A. Then the observer to take K_B and k_A and compute the shared secret too.

13. (12 pts) Consider the Unix password authentication system discussed in class and in the text.
    a. What is the complementation information stored on the file system?

The complementation information in this case is the hash of the password string.

    b. What information does the attacker need to perform a type 1 or offline attack?

He needs the complementation information and the associated account names.

    c. What is one benefit of salting?

It in creases the computational cost of performing an offline attack. Instead of computing the hash once for each password guess, the attacker must compute the hash for each salting variation in the target password file set.

    d. Given passwords of length 8, an alphabet size of 26, and an opponent capable of checking 15000 passwords a second. Set up Anderson's equation to compute the probability that a password will be found after 30 days.

$P = T*G/N = (30*24*60*60)*15000/(26^8)$