Net ID:

University of Illinois at Urbana-Champaign
Department of Computer Science

Midterm 1 – Answers and Comments
CS461/ECE422 – Computer Security I
Fall 2009
Wednesday, October 7, 2009
Time Limit: 50 minutes

Multiple Choice – 3 points each

1. Which of the following is a problem with output feedback mode algorithms such as Schneier's Solitaire encryption scheme?
    a. Predictable key stream generation
    b. Lack of reliable crypto-analysis schemes.
    c. Presence of patterns in resulting cipher text that are vulnerable to language analysis.
    d. Loss of synchrony between the ciphertext stream and the key stream

2. Which of the following cryptographic algorithms do **not** include transposition?
    a. Vigenere's encryption
    b. Rail cipher
    c. AES
    d. DES

3. You read that someone have found an efficient algorithm for computing the factors of large numbers. Which algorithm would you want to stop using immediately?
    a. RSA
    b. Diffie-Hellman
    c. AES
    d. Bin packing

4. Which algorithm would be most appropriate for computing a verification of files stored on a mirrored download site?
    a. CRC
    b. SHA-256
    c. DES-CBC
    d. HMAC-SHA1

5. Which is the best definition of a totient function, Φ(n)?
    a. The modulus of the RSA key pair.
    b. *The number of numbers less than n with no factors in common with n.*
    c. The number of numbers less than n that are factors of n.
    d. The largest number less than n that is a factor of n.

6. In which case is salting a password beneficial for preventing attack on passwords?
    a. Preventing an online attack against an individual's account.
    b. Preventing an offline attack against an individual's account.
    c. Preventing an online attack against any account.
    d. Preventing an offline attack against any account.

7. Consider the following statement: "All individuals attempting to access UIUC's recreation facilities must present valid UIUC IDs upon entrance." Which of the following is true about it?
    a. It is a mechanism since it identifies the purpose of protection.
    b. It is a mechanism and is presumably implementing a policy that restricts access to UIUC recreation facilities to registered UIUC students.
    c. It is a policy since it identifies the object being protected and the purpose of protection.
    d. It is a policy since its implementation is not straightforward.

Net ID:

8. (10 points) The table below includes a number of steps involved in quantitative and qualitative risk analysis. Fill the empty cells as follows:
    a. Mark each step as being in the category of the quantitative analysis (QT) or qualitative analysis (QL) processes (discussed in class) in column 2.

    b. Determine the order in which the identified steps should be performed in their respective category. For example, if you think "Calculate Risk Leverage to evaluate value of control" is the first step (*among the mentioned steps*) in quantitative or qualitative analysis, put #1 in column 3. Please note that we do not provide a comprehensive list of steps, so the numbering is relative. Start with #1 as the first step in each category.

    For this step most people numbered 1-5. We evaluated the relative ordering within each category (QT or QL).

Step	QT or QL?	Relative Step Number
Sum up the threat priority and impact priority to determine risk factor	*QL*	*3*
Calculate Annual Loss Exposure (ALE)	*QT*	*1*
Prioritize threats for each asset with a fixed ranking from low to high	*QL*	*2 or 1*
For each threat determine loss impact with a fixed ranking from low to high	*QL*	*1 or 2*
Calculate Risk Leverage to evaluate the value of control	*QT*	*2*

9. (5 pts) Use the text from question 10 (starting after the point identification) and the Vigenere's tableau at the end of the exam (if needed) to encrypt the following phrase using the book cipher technique.

    CRYPTO IS FUN

Key is ALICEANDBOB from question 10
Ciphertext is `CCGRXOVVGIO`

Most got this. A few used Q8 above for the key and lost a couple points.

10. (8 points) Alice and Bob are passing messages encrypted with DES. C = DES-Encrypt(K, M)
    a. If Eve obtained a plaintext/ciphertext pair, how many cryptographic operations would she need to perform to find Alice and Bob's shared key K?

2^56 encrypt or decrypt operations

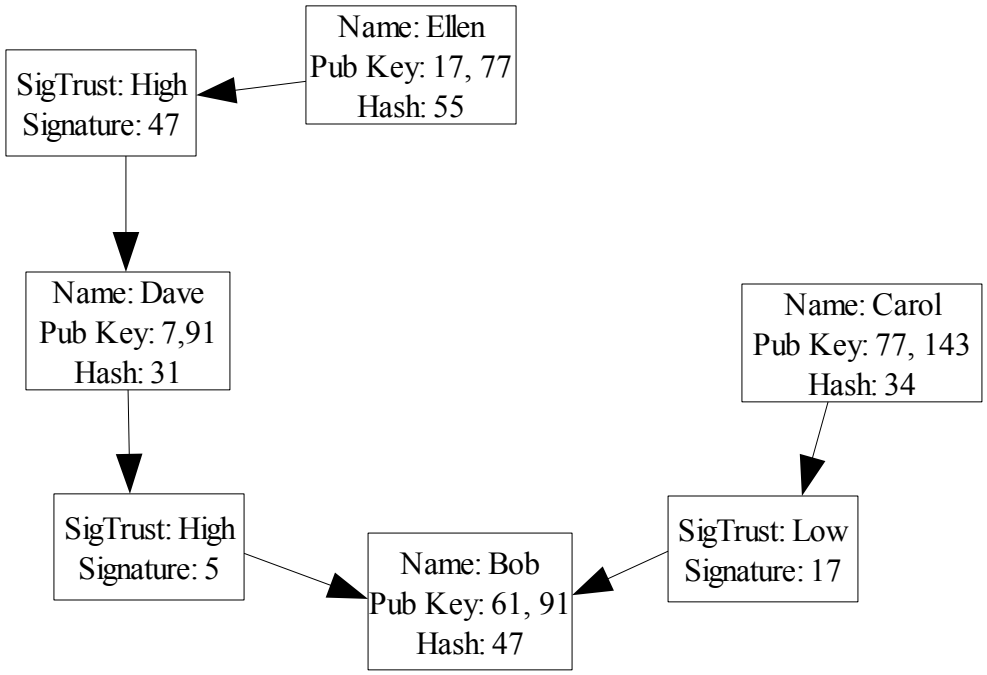
    b. Alice and Bob dimly remember that double encrypting with the same algorithm doesn't provide much additional protect. Alice suggested using the NOTDES algorithm which operates with a 32 bit key with the DES algorithm, i.e. C = NOTDES-Encrypt(K1, DES-Encrypt(K2, M)). If Eve has a plaintext/ ciphertext pair, how many cryptographic operations would she need to perform to recover the keys?

Meet in the middle still works. The attacker would brute force the DES key performing 2^56 encryptions. The attacker would in addition perform a NOTDES decrypt using the first (or last or some fixed subset of) 32 bits in the current 56 bit key.

Results in 2^57 encrypt/decrypt operations. Or 2^56 + 2^32 encrypt/decrypt operations if we are being clever about not rechecking if the selected 32 bits in the current 56 bit key have been checked.

Net ID:

11. (16 points) The signature relationships on Bob's GPG certificate are shown below. Each certificate is identified with a box. Signatures are identified by arrow connected boxes. You already have Ellen's and Carol's certificates verified on your local machine. The public keys in all the certificates are RSA keys.



Questions on next page

a. Write the equations you would solve in verifying Carol's signature of Bob's certificate.

Bob's hash = Carol's sig ^ 77 mod 143
47 = 17 ^ 77 mod 143

Should also recompute Bob's hash and make sure the computed value matches the stored value.

b. Which chain of signatures gives you the best proof of Bob's certificate? Why?

The Ellen-Dave-Bob chain because each of those signatures has a high level of trust. The other chain is shorter but the signature is at a lower level of trust.

c. Assume you did not have Carol's certificate verified on your local machine before receiving Bob's certificate. What attack could Eve launch if you tried to verify Carol's signature on Bob's certificate?

When asking for Carol's certificate from a server or a neighbor, Eve could pretend to be Carol, and return her certificate instead of Carol's. Then if Eve could give you certificates that are signed with her version of Carol's key pair.

d. Give a reason why it is better to sign a hash of a message rather than signing a message directly.

Performance. Asymmetric encryption operations are expensive. Better to encrypt the smaller hash.

Security. Makes it impossible (or more difficult) to play games with the message and the mathematical properties of the asymmetric algorithm, like the RSA message multiplications discussed in class.

Error detection. In addition to authentication of the message, your hash provides error detection against the message.

Net ID:

12. (12 points) You are tasked with designing a challenge response authentication system.
    a. Propose a response f function.

A number of options: one time password list. Present a value based on the time. Encrypt a challenge nonce using a common encryption algorithm and common key. Even a fairly simple minded function like f(x) = x – 1 would satisfy the requirements, but obviously wouldn't be a good function in real life.

A number of folks proposed passwords and/or security questions. The challenge should change each time, so these answers were not fully satisfactory.

A number of other folks proposed captcha systems. This isn't really an individual authentication system. It classifies individuals into probably human and probably bot. You couldn't distinguish alice and bob using a captcha system.

    b. What information do the challenger and responder need to share ahead of time?

Depends on the answer to part a. The list of passwords, the list of time stamps and replies. The common encryption key. Or perhaps just details of the function.

    c. What is one limitation of your approach?

Long lists and need to synchronize for the one time password. Revealing plaintext/ciphertext pairs over the wire for the encrypted nonce approach. Deducing the secret function over time.