CS255: Cryptography and Computer Security **Winter 1998**

Final Exam

Instructions
− Answer **four** of the following six problems. Do not answer more than four.
− The exam is open book.
− You have two hours.

Problem 1 Properties of CBC mode encryption.

Alice and Bob share a secret key k. Alice encrypts a long message M in CBC mode and sends the resulting ciphertext, C, to Bob. Say the cipher block size is 64 bits (as in DES).

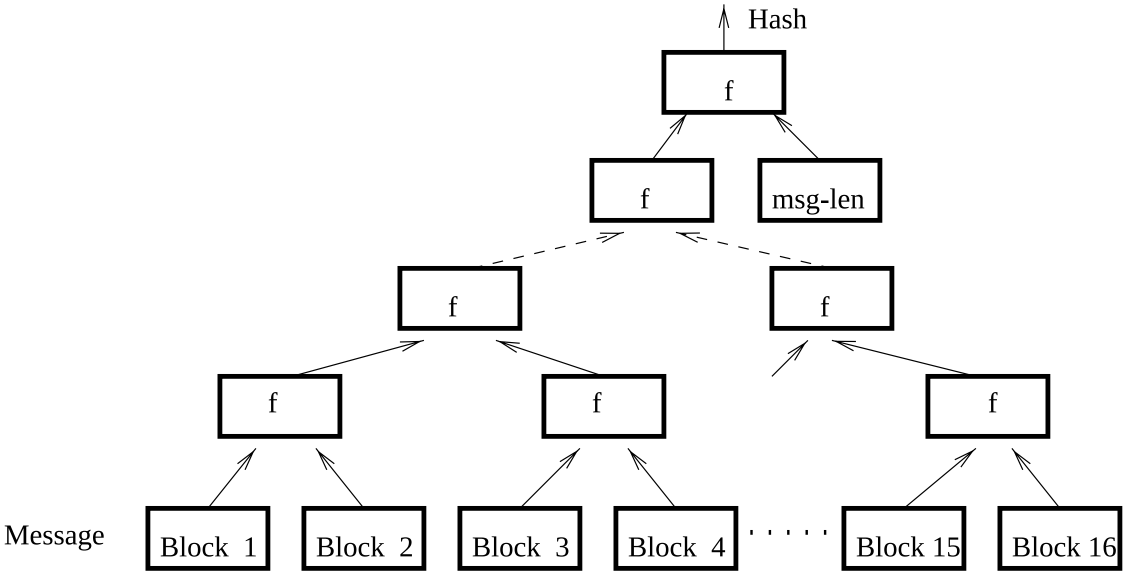
A. Suppose that due to a transmission error Bob receives a message C' which differs from C in one bit position. What is the maximum number of erroneous bits that will be present in the plaintext after Bob decrypts C'?

B. Suppose that due to a transmission error Bob receives a message C' which is identical to C except that an extra bit is inserted at some point. That is, C' is one bit longer than C, but otherwise identical to it. What is the maximum number of erroneous bits that will be present in the plaintext after Bob decrypts C'?

C. What is the purpose of the IV used in CBC mode? Why is it not simply set to zero? For simplicity, consider the case where the IV is kept secret as part of the key.

Problem 2 Merkle hash trees.

Merkle suggested a parallelizable method for constructing hash functions out of compression functions. Let f be a compression function that takes two 512 bit blocks and outputs one 512 bit block. To hash a message M one uses the following tree construction:



Prove that if one can find a collision for the resulting hash function then one can find collisions for the compression function.

Problem 3 Dining cryptographers — anonymous broadcast.

Three cryptographers were eating dinner at a restaurant when the waiter informed them that their meal has been paid for. They were very curious to know if one of them paid for the meal, or someone else did. Being cryptographers, they agreed that even if one of them paid for the meal, the party's identity should remain private. They agree to run the following protocol:

1. Each of the three flips an unbiased coin keeping the result r_i secret.
2. They each whisper the result in the ear of the person to their immediate right.
3. Each cryptographer computes $b_i = r_i \oplus r_{i-1}$ where r_i is the person's own coin flip and r_{i-1} is the coin flip of the person on the left.
4. A cryptographer that did not pay for the meal announces her own b_i. In case one of the cryptographers paid for the meal that cryptographer announces the negation of b_i, i.e. $b_i \oplus 1$.

A. Show that if the xor of the three announced values is zero then someone else paid for the meal. Otherwise, one of the three paid for it.

B. Show that if the answer is one then any of them who did not pay for the meal, has no idea which of the other two did. If you can, argue that given all the information that cryptographer A has, the probability that cryptographer B paid for the meal is exactly one half.

C. Can this protocol be applied when more than three parties are involved?

D. Observe that (in theory) this protocol can be used to provide anonymous broadcast.

Problem 4 Questions about RSA.

A. Let p be a prime with $p = 2 \bmod 3$. Show that given $\alpha \in \mathbb{Z}_p^*$ one can efficiently find the cube root of α modulo p. That is, one can solve the equation $x^3 - \alpha = 0 \bmod p$.
Hint: recall how RSA decryption works.

B. Is your algorithm from part A able to compute cube roots modulo a composite $N = pq$ when the factorization of N is unknown? If so, prove it. If not, describe an alternate algorithm or explain why you believe no such efficient algorithm exists.

C. Some proposals suggest making the RSA modulus a product of three primes $N = pqr$ of equal size. Describe the RSA system in this case. That is, explain how e and d are chosen.

D. Explain why using products of three primes may be a good idea. Think of the running time of the decryption process when the Chinese Remainder Theorem (CRT) is used. Compare the decryption time when $N = pq$ is used and when $N' = p'q'r'$ is used. Assume both N and N' are 1024 bits long.
Hint: recall that to compute $M^d \bmod p$ it suffices to compute $M^{d \bmod p-1} (\bmod\ p)$ resulting in a potentially much smaller exponent.

Problem 5 Anonymous remailers

A serious problem with anonymous cash is the network: when Alice connects to the vendor through the Internet, the vendor knows her IP address. If the network reveals Alice's identity there is no point to using anonymous cash. To solve the problem, Chaum introduced the notion of a *mix*.

The basic idea is for Alice to communicate with the vendor through a small number of relays. Even if some (but not all) of these relays are operated by the FBI, there should be no way to tell that Alice is communicating with vendor Bob. Each of the relays has a public key known to Alice and the vendor, and a private key known only to the relay. When Alice sends out a message, the relays pass the message in a chain from one to the other until the last relay sends it to Bob.

Design a scheme that enables Alice to send messages to vendor Bob and enables Bob to respond without knowing who Alice is. Alice is allowed to embed extra information in the message she sends to the first relay. Each relay is allowed to process the message in turn. For privacy, you may assume Alice has vendor Bob's public key. Also, you may assume the relays process millions of messages a second so that traffic analysis attacks are not possible. Relays only send messages. They do not keep any connections open nor do they have any state. Again, you must make sure that even if some relays are captured by an adversary there is still no way to tell that Alice is communicating with Bob. Such a system was built at NRL.

Hint: Alice's goal is to make sure each relay knows the ID of the next relay in the chain, but no other relays further along in the chain.

Problem 6 Questions from all over.
Answer each of the following questions with a four line answer *at most.*

A. Explain the difference between a signature and a MAC. Can one be used in place of the other?

B. In a hash-then-sign signature scheme, how long will it take to create some forged valid (message,signature) pair if the signature is 80 bits long.

C. Briefly explain the purpose of certificate chains.

D. A server can authenticate a remote workstation by asking it to sign a random message. Why is this method worse than a customized authentication protocol, such as Fiat-Shamir?

E. When designing the security component of a large system, should you use an off the shelf standardized cipher, or design your own proprietary one? This is not a trick question.