

Homework 3

Due: March 12, 2009, 10:00 PM EST

Please hand in your solutions as a pdf document

Problem 1 In class we have discussed how to use a *hash tree* to create proofs of membership for the elements of a set D . Alternatively, the *sign-all* approach to membership proofs is as follows.

For each element $e \in D$, Alice signs e and stores the signature. When the membership of an element x is queried by Bob, Alice returns the signature of x . Bob verifies this signature using Alice’s public key.

Compare the sign-all approach with the hash-tree approach by analyzing the complexity of the following protocol:

1. Alice creates and stores membership proofs for the n elements of a set. Each element has constant size.
2. Bob queries the membership of k elements.
3. Alice returns the k proofs of membership of these elements.
4. Bob verifies the k proofs.

In particular, for each step of the protocol, analyze the following cost measures (as a function of n and k) for the sign-all approach and the hash-tree approach.

- *hash complexity*: total size of the data hashed;
- *signature complexity*: number of signature operations;
- *verification complexity*: number of signature verification operations;
- *communication complexity*: total size of the data transmitted by one party to the other party.

Problem 2

- What is the difference between the ECB and CBC modes for a symmetric block cipher? Suppose we are using a symmetric block cipher under CBC mode to encrypt n 64-bit blocks B_1, B_2, \dots, B_n . Suppose there is a bit error in the source version of B_i . Which ciphertexts are affected? What is the effect at the receiver (i.e., during decryption)?
- A message authentication code (MAC) is a piece of information used to authenticate a message. To compute a MAC, a secret key k and an arbitrary-length message x are used as input. The MAC value protects the integrity of the message allowing recipients who also possess the secret key to detect any changes to the message content. For example, we can use a collision-resistant cryptographic hash function h to construct the MAC $y = h(k||x)$, where k is the secret key, x is the plaintext message, and $||$ denotes concatenation. Assuming that the sender and recipient know secret key k ,

message x is transmitted together with MAC y . The recipient recomputes the MAC from the received message and compares it with the received MAC.

We describe now a MAC construction that uses a symmetric block cipher. Let $E_k()$ be the encryption function of a block cipher, where k is the secret key. Suppose message x consists of n blocks $x_1||x_2||\dots||x_n$ and let $r_i = x_1||x_2||\dots||x_i$. We define MAC function $Q_k(x)$ as follows:

$$\begin{aligned} Q_k(r_1) &= E_k(x_1) \\ Q_k(r_i) &= E_k(Q_k(r_{i-1}) \oplus x_i) \text{ for } i = 2, \dots, n \\ Q_k(x) &= Q_k(r_n) \end{aligned}$$

Describe a possible attack when this MAC function is used for variable-length messages. The adversary is allowed to intercept pairs of messages and MACs (Hint: You should try to find a replay attack, where the attacker constructs another message and its MAC without knowing secret key k).

Problem 3 Let $E_K(\cdot)$ and $D_K(\cdot)$ be the encryption and decryption algorithms of a symmetric key cryptosystem with ℓ -bit keys and n -bit plaintexts and ciphertexts. We derive another symmetric key cryptosystem with 2ℓ -bit keys by applying twice $E_K(\cdot)$ and $D_K(\cdot)$:

$$\begin{aligned} E'_{(K_1, K_2)}(M) &= E_{K_2}(E_{K_1}(M)) \\ D'_{(K_1, K_2)}(C) &= D_{K_1}(D_{K_2}(C)) \end{aligned}$$

Consider an adversary that wants to perform a brute-force attack on the above cryptosystem to recover keys K_1 and K_2 but knows only a single valid pair of plaintext M and ciphertext C .

1. Suppose that the adversary has only $O(1)$ space. Describe the attack in pseudo-code and estimate the number of encryption and decryption operations performed.
2. Suppose now that the adversary has $O(2^\ell)$ space. Describe a more efficient way to perform the attack and estimate the number of encryption and decryption operations performed.
3. Can there be more than one pair of keys that map plaintext M to ciphertext C ? Justify your answer.

Problem 4 In `/course/cs166/asgn/hw3` there are two files: `passwords` and `dictionary`. Your task for this assignment is to use the dictionary to conduct an attack against the provided password file and glean your password. The MD5 hash function is what we used and is available. e.g., via command `md5sum`. Please include the source code with your handin.

1. What is your password?
2. Describe two defenses against dictionary attacks on password files.