Homework #2 for CS 419— Computer Security

1 Flipping Attack

Read Bit-flipping attack: `https://en.wikipedia.org/wiki/Bit-flipping_attack`

Please explain how to perform such attacks on AES using CBC mode, and discuss the root cause and potential defenses.

2 RSA and RSA Signature

In this problem, please use RSA encryption scheme and signature scheme to calculate the following concrete instance, where the public key is $N = 91$ and secret key(factoring) is $(7, 13)$:

1. let $e = 5$, please calculate the corresponding secret key d.
2. let $\mathsf{M}_1 = 8$, please calculate the ciphertext $\mathsf{Enc}(\mathsf{pk}, \mathsf{M}_1)$.
3. let $\mathsf{M}_2 = 17$, please calculate the signature $\mathsf{Sign}(\mathsf{sk}, \mathsf{M}_2)$.

3 Diffie-Hellman Key Agreement Protocol

In Diffie-Hellman protocol, two clients "Alice" and "Bob" share their secret key as follows:

- Alice has public key g^a and secret key a;
- Bob has public key g^b and secret key b;
- Once they get each other's public key, they calculate the shared secret key g^{ab} individually.

To argue its security, we first formalize two types of adversary: *passive adversary* and *active adversary*. The passive adversary only eavesdrop, say it only has the two public keys g^a and g^b and the goal of the passive adversary is to output g^{ab}. On the contrary, the active adversary has additional power, essentially it can picks a well-formed public keyg^c (where c is uniformly distributed) and sends g^c to Alice (or Bob), then Alice(or Bob) would give back the shared key g^{ac}(or g^{bc}) to the active adversary. Same as above, the goal of the active adversary is also to output the shared key g^{ab}.

1. Please give an intuitive explanation that Diffie-Hellman key agreement protocol is secure against the passive adversary under Computational Diffie-Hellman assumption.
2. Please design an attack, by showing how an active adversary breaks the Diffie-Hellman key agreement protocol.

4 IND-CPA

When we say an encryption is randomized, we means that during the encryption, some randomness are involved. And different randomness, even under the same secret key and message, would reduce to different ciphertext. On the contrary, when we say an encryption is deterministic, it means that $\mathsf{Enc}(\mathsf{sk}, \mathsf{m})$ are fixed, under the same secret key and message.

Please prove that: IND-CPA implies that the encryption is randomized.

Hint: Try to find an attack in the CPA game if the encryption is deterministic.

5 Web Security: SQL Injection

Please try to solve RedTiger's SQL Injection challenges. Please record your solutions in details here. Important: DO NOT SHARE YOUR SOLUTIONS.

`https://redtiger.labs.overthewire.org`