Problem Set 2

This problem set is due on *Thursday, September 28* at the end of class.

Each solution is to be handed in *separately*, i.e. on separate sheets of three-hole punched paper. If the solution to a single problem takes more than one page, staple together only the pages relative to the same problem. Mark the top of each sheet with your name, 6.915, the problem number, and the date.

If you collaborate with other students, you MUST write up solutions on your own and acknowledge the people you work with.

Readings: Chapters 2 and 3 of textbook

Problem 2-1. DES

Let $\bar{m}$ be the bitwise complement of the string m. Let $\mathrm{DES}_K(m)$ denote the encryption of m under DES using key K.

(a) Prove that if

$$c = \mathrm{DES}_K(m)$$

then

$$\bar{c} = \mathrm{DES}_{\bar{K}}(\bar{m})$$

We know that a brute–force attack on DES requires searching a space of 2^{56} keys. This means that we have to perform that many DES encryptions in order to find the key, in the worst case.

(b) Under *known plaintext attack* (i.e., you are given a single pair (m, c) where $c = \mathrm{DES}_K(m)$) does the result of part (a) change the number of DES encryption you perform in a brute–force attack to recover K?

(c) What is the answer to the above question in the case of *chosen plaintext attack* (i.e., when you are allowed to choose many m's for which you get the pair (m, c) with $c = \mathrm{DES}_K(m)$)?

Problem 2-2. Message authentication codes

In class we introduced the concept of message authentication codes (MACs.) Alice and Bob share a secret key k. Bob wants an assurance that the message he receives are really coming from Alice. In order to obtain this Alice sends the message m and a MAC along with it $\mathrm{MAC}_k(m)$.

We say that a MAC is secure against *chosen message attack* if an attacker Eve, after requesting the MAC $\mathrm{MAC}_k(m_i)$ of n messages of her choice $m_1, \ldots, m_n$ will not be able to produce a *new* message $m \neq m_i$ and a valid $\mathrm{MAC}_k(m)$.

Let us CBC-MAC a way of implementing MACs using symmetric encryption scheme. Let

$$f_k : \{0,1\}^\ell \to \{0,1\}^\ell$$

be an encryption function with key k (for example with $\ell = 64$, f could be DES.) Let m be a message of length $b\ell$ bits.

$$m = m_1 \circ \ldots \circ m_b$$

where $\circ$ denotes concatenation and m_i is a block of length ℓ bits. The MAC of m is computed using the cipher f in CBC mode:

$$\mathrm{MAC}_k(m) = f_k(f_k(\ldots f_k(f_k(m_1) \oplus m_2) \oplus \ldots m_{b-1}) \oplus m_b)$$

(a) Show that the CBC–MAC does not support variable length input. That is show that if messages have variable length it is possible to device a chosen message attack.

Hint: The idea is to ask for the MACs of two messages of length ℓ and construct from them the MAC of a message of length 2ℓ.

(b) Suppose the length of the messages is always smaller than 2^ℓ. An attempt to get around the above problem would be to append the length of the message at the end as an extra block, before computing the MAC. Show that it is still possible to mount an effective chosen message attack.

Problem 2-3. Protocol Failure involving RSA

Remember that an RSA public–key is a pair (n, e) where n is the product of two primes.

$$RSA_{(n,e)}(m) = m^e \bmod n$$

Assume that three users in a network Alice, Bob and Carl use RSA public–keys $(n_A, 3)$, $(n_B, 3)$ and $(n_C, 3)$ respectively. Suppose David wants to send the *same* message m to the three of them. So David computes

$$y_A = m^3 \bmod n_A \ , \ y_B = m^3 \bmod n_B \ , \ y_C = m^3 \bmod n_C$$

and sends the ciphertext to the relative user.

Show how an eavesdropper Eve can now compute the message m even without knowing any of the secret keys of Alice, Bob and Carl.

Problem 2-4. Perfect Forward Secrecy

Suppose two parties Alice and Bob want to communicate privately. They both hold public keys in the traditional Diffie-Hellman model.

An eavesdropper Eve stores all the encrypted messages between them and one day she manages to break into Alice and Bob's computer and find their secret keys, correspondent to their public keys.

Show how using only public–key cryptography we can achieve *perfect forward secrecy*, i.e., Eve will not be able to gain any knowledge about the messages Alice and Bob exchanged before the disclosure of the secret keys.