CS255: Cryptography and Computer Security **Winter 1999**

Assignment #1

Due: Wednesday, January 27th, 1999.

Problem 1 Data compression is often used in data storage or transmission. Suppose you want to use data compression in conjunction with encryption. Does it make more sense to

A. Compress the data and then encrypt the result, or

B. Encrypt the data and then compress the result.

Justify your answer. Try to give at least two reasons.

Problem 2 Before DESX was invented, the researchers at RSA Labs came up with DESV and DESW, defined by

$$\begin{aligned} DESV_{kk_1}(M) &= DES_k(M) \oplus k_1 \text{ and} \\ DESW_{kk_1}(M) &= DES_k(M \oplus k_1) \end{aligned}$$

As with DESX, $|k| = 56$ and $|k_1| = 64$. Show that both these proposals do not increase the work needed to break the cryptosystem using brute-force key search. That is, show how to break these schemes using on the order of 2^{56} DES encryptions/decryptions. You may assume that you have a moderate number of plaintext-ciphertext pairs, $C_i = DES\{V/W\}_{kk_1}(M_i)$.

Problem 3 Given a cryptosystem E_k, define the randomized cryptosystem F_k by

$$F_k(M) = (E_k(R), R \oplus M),$$

where R is a random bit string of the same size as the message. That is, the output of $F_k(M)$ is the encryption of a random one-time pad along with the original message XORed with the random pad. A new independent random pad R is chosen for every encryption.

We consider two attack models. The goal of both models is to reconstruct the actual secret key k.[1]

- In the key-reconstruction chosen plaintext attack (KR-CPA), the adversary is allowed to generate strings $M_1, M_2, \ldots$ and for each M_i learn a corresponding ciphertext.
- In the key-reconstruction random plaintext attack (KR-RPA), the adversary receives random plaintext/ciphertext pairs.

Note that for the case of F_k the opponent has no control over the random pad R used in the creation of the given plaintext/ciphertext pairs.

Prove that if E_k is secure against KR-RPA attacks then F_k is secure against $\mathsf{KR-CPA}$ attacks.

[Hint: It is easiest to show the contrapositive. Given an algorithm A that executes a successful $\mathsf{KR-CPA}$ attack against F_k, exhibit an algorithm B (using A as a "subroutine") that executes a successful $\mathsf{KR-RPA}$ attack against E_k.]

[1] This is a very strong goal - one might be able to decrypt messages without ever learning k.

Problem 4 Let $E(M, k)$ be a block cipher using 56-bit keys. Suppose Alice sends the ciphertext $C_1 = E(M_1, k_1)$ to Bob and sends the ciphertext $C_2 = E(M_2, k_2)$ to Charlie. An eavesdropper, Eve, intercepts the two ciphertexts C_1 and C_2. Suppose Eve knows $\Delta = M_1 \oplus M_2$.

Eve's goal is to find k_1 and k_2. Assume the messsages M_1 and M_2 are sufficiently long that given C_1, C_2 and Δ the pair of keys (k_1, k_2) is uniquely determined. By trying all possible pairs of keys Eve can find (k_1, k_2) using 2^{112} applications of the decryption function (simply try all k_1', k_2' until a pair satisfying $D(C_1, k_1') \oplus D(C_2, k_2') = \Delta$ is found).

Show that given C_1, C_2 and Δ Eve can find (k_1, k_2) using only 2^{57} application of the decryption function. Your algorithm may use as much memory space as you wish.

Extra credit Show that if all the S-boxes in the DES cipher are replaced by an identify function (i.e. given a six-bit input the function outputs the four least significant bits) then the resulting cipher is easily broken. In other words, show that given a few plaintext/ciphertext pairs the an attacker can quickly recover the secret key.