Cryptography (SS2006) Prof. Michael Backes

Exercise Sheet 2

Out: May 2, 2006 Saarland University

Problem 1 (Key Complementarity of DES)

(a) Show that in the DES structure, $\overline{\mathsf{E}^{\mathsf{DES}}(K,m)} = \mathsf{E}^{\mathsf{DES}}(\overline{K},\overline{m})$, where $\overline{x}$ denotes the bitwise complement of x and $\mathsf{E}^{\mathsf{DES}}(K,m)$ is the DES encryption function using key K and message m.

(b) Show how an attacker can use this fact in order to speed up the exhaustive key search for DES by roughly a factor of 2. Try to be precise in which assumptions you make (on the capabilities of the attacker, speed of DES as opposed to other operations, etc.) to claim your speedup.

Problem 2 (DESV and DESW)

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

$$\mathsf{E}^{\mathsf{DESV}}((K,K_1),m) = \mathsf{E}^{\mathsf{DES}}(K,m)\oplus K_1 \quad \text{and} \quad \mathsf{E}^{\mathsf{DESW}}((K,K_1),m) = \mathsf{E}^{\mathsf{DES}}(K,m\oplus K_1),$$

decryption is defined in the obvious way. Similar to DESX, $|K| = 56$ and $|K_1| = 64$. Show that both these proposals do not increase the work needed to break DES using brute-force key search. Show that breaking these schemes is possible in roughly 2^{56} DES encryptions/decryptions (up-to small computational overhead). You may assume that you have a moderate number of plaintext-ciphertext pairs, $c_i = \mathsf{E}^{\mathsf{DES\{V/W\}}}((K,K_1),m_i)$.

Problem 3 (DES Simplification)

Let $K_1,\dots,K_{16}$ be 16 random values in $\{0,1\}^{32}$. Suppose the 16 round functions $f_1,\dots,f_{16} : \{0,1\}^{32} \to \{0,1\}^{32}$ used in DES were simply defined as

$$f_i(x) = x \oplus K_i.$$

The key for the resulting cipher is $\hat{K} = (K_1,...,K_{16})$ and its size is $16\cdot 32 = 512$ bits. Show that the resulting cipher is universally breakable. More precisely, suppose we are given a few plaintext/ciphertext pairs $(m_i,\mathsf{E}(\hat{K},m_i))$, say for $i = 1,\dots,10$, where the m_i are chosen randomly in $\{0,1\}^{64}$. Show how to use this data to decrypt any ciphertext, i.e., given any $\mathsf{E}(\hat{K},m)$, show how to recover m.

Problem 4 (Two-key Triple DES)

One variant of triple encryption with DES using two rather than three 56 bit keys is the following:

$$c = E(K_1,E(K_2,E(K_2,m)))$$

Show that this cipher succumbs to a meet-in-the-middle-attack (spell out the details, i.e., write down the sets/lists you compute and between which you look for overlap); how much time/space does the attack need?