Secret Key Cryptography (Spring 2004)

Instructor: Adi Shamir Teaching assistant: Eran Tromer

Lecture notes: DES

1 Background

- Until early 1970's: little cryptographic research in industry and academcy. Cryptographic equipment used by industry is non-interoperable and has dubious security.
- 1973: NBS (National Bureau of Standards, U.S.A.) issues public call for general-purpose encryption algorithm.
- One of the NBS criteria: the security must rely on the secrecy of the key, not of the algorithm (Kerckhoff's rule). Today widely accepted in academy and industry; rationale:
  - The algorithm is fixed, and will eventually be discovered, so it is folly to rely on its secrecy.
  - ... and thus we might as well reveal it in advance, to get peer review from the "good guys".
- No submission met NBS criteria. Call re-issued in 1974. This time IBM made a promising proposal. Modifications made by NSA (National Security Agency, U.S.A.): decreased key size from 128bit to 56bit, and some other mysterious changes (mostly understood today, in retrospect)
- 1976: following much public discussion, and despite concerns over the NSA's involvement, the revised proposal was accepted as Data Encryption Standard (DES). Later accepted by other standard bodies.
- DES is the first noteworthy published modern cipher. It spurred enormous cryptanalitic interest, by provding a real challenge. It marks the beginning of (civilian) modern cryptography.

2 Stream ciphers vs. block ciphers

Stream cipher	Block cipher
• Encrypts streams of arbitrary size, one bit/character at a time. • Stateful: initialized using key, and evolves at every step. • Low latency (single bit/character). • Usually faster/cheaper in hardware implementation (e.g., mobile phones), sometimes at the cost of security.	• Encrypts fixed-size block (usually 64bit or 128bit) • No state. • High latency (full block). • More popular for computer communication and data storage.

3 Structure and properties of DES

See bibliography links in the course website for detailed sescriptions. The notation L_i and R_i below follow those of the Handbook of Applied Cryptography. Some notes:

- DES is a 16-round Feistel network. Decryption comes "for free" from the Feistein structure, regardless of the F rounf function: it is identical to encryption, except that the key schedule is reversed.
- The initial permutations IP, IP^{-1} and PC-1 are vestiges of ancient hardware considerations. They do not affect security, and can be ignored.
- The only non-linear component is the S-boxes in the F function. If it weren't for these, the whole function would be linear and could be broken by obtaining a (plaintext,cihpertext) pair and solving a system of linear equations.
- E and P help achieve the avalance effect: every bit of the plaintext affects quickly affects many bits of L_i, R_i.
- Note that sum of shifts is 28, so the key returns to its original state in time for the next block encryption.
- DES has 4 "weak keys": keys K such that $\mathrm{DES}_K(\mathrm{DES}_K(p)) = p$. Susceptible to chosen-plaintext attack (recall the WWII Enigma story). There are also 6 "semi-weak" keys.
- Complementarity property of DES: $DES_{\bar{k}}(\bar{p}) = \overline{DES_k(p)}$.

Exercise 1. Prove the complementarity property of DES: $DES_{\bar{k}}(\bar{p}) = \overline{DES_k(p)}$.

4 Simple attacks on DES reduced number of rounds

Let $\text{DES}^{(r)}$ denote DES with r rounds instead of the usual 16 rounds.

- Known-plaintext attack on $\text{DES}^{(1)}$:
  - Consider some known (plaintext,ciphertext) pair.
  - We know the input and output of F: $F_{K_1}(R_0) = L_0 \oplus L_1$.
  - By following E and P, for each S-box $i \in \{1, \ldots, 8\}$ we get an equation $S_i(K_{1,i} \oplus a_i) = b_i$.
  - For each $i \in \{1, \ldots, 8\}$, try all possibilities for $K_{1,i}$ (i.e., the 6 key bits entering Si). The correct value will fulfill the equation. For a bad guess $K'_{1,i}$, $S_i(K'_{1,i} \oplus a_i)$ will be "random" and will thus fulfill the equation with probability just 2^{-4}.
  - Each additional (plaintext,ciphertext) pair yields another set of equations. Thus, after 2 or three pairs only one possibility will remain for each subkey $K_{1,i}$.
- Known-plaintext attack on $\text{DES}^{(2)}$: we have $F_{K_1}(R_0) = L_0 \oplus R_2$, so the above attack can still be carried out to recover K_1. We can recover the remaining $56 - 48 = 8$ key bits by exhaustive search; alternatively, note that we know the inputs and outputs of F in round 2, $F_{K_2}(R_2) = R_0 \oplus L_2$, and can thus carry out an an analogous attack to recover the subkey K_2.
- Known-plaintext attack on $\text{DES}^{(3)}$:
  - For the second round, we know the output (R_3) of F_{K_2} but not the input R_2.
  - Consider $S6$ in round to, and the associated key bits $K_{2,6}$. To obtain equations on $S6$ in round 2, we need to know the 6 bits of R_2 that enter $S6$. By E, these are bits 20,21,22,23,24,25.
  - $R_2 = L_1 \oplus F_{K_1}(R_1)$, so it suffices to know bits 20,21,22,23,24,25 of $F_{K_1}(R_1)$. By applying P^{-1}, we see that these are bits 3,4,29,11,19,32 of $P^{-1} \circ F_{K_1}(R_1)$, which are outputs of S-boxes $1, 3, 5, 8$ in round 1.
  - Guess (that is, try all possibilities) all of $K_{1,1}, K_{1,3}, K_{1,5}, K_{1,8}$ and $K_{2,6}$. These are just 26 bits (not $5 \cdot 6 = 30$), since $K_{2,6}$ shares 3 bits with $K_{1,5}$and 1 bit with $K_{1,8}$ — to see this look at the table of PC-2 and note the rotate-left-by-1 key schedule operation. For each guess compute the inputs to $S6$ of round 2 and check if the output is correct. An incorrect guess will fail with probability $\frac{3}{4}$.
  - Check additional (plaintext,ciphertext) pairs, and for each see if the equation for $S6$ of round 2 holds. Each pair reduces the number of consistent choices of $K_{1,1}, K_{1,3}, K_{1,5}, K_{1,8}, K_{2,6}$ by a factor of 2^4, so after only about $2^{26}/2^{-4 \cdot 8}$ (i.e., probably zero) bad keys will remain.

– Do the same for two more S-boxes (making use of the partial knowledge already available) to recover the rest of the key.

Exercise 2.

a. Suppose you have a distinguisher for $\mathrm{DES}^{(15)}$: an algorithm that, given a pair (c, p), says whether there exists some key K such that $\mathrm{DES}^{(15)}_K(p) = c$. Show an efficient known-plaintext attack on $\mathrm{DES}^{(16)}$ which recovers the subkey of the last round.

b. Extend the previous attack to recover the full key of $\mathrm{DES}^{(16)}$.

5 Current security of DES

- Susceptible to Hellman time/memory trade-off.
- Linear and differential attacks: time complexity reduced to 2^{43}, but enormous amounts of known or chosen plaintexts. Will be discussed in future lectures.
- Exhaustive search: Electronic Frontier Foundation "DES Cracker" dedicated hardware machine, US$210,000 in 1998, breaks a DES key in a couple of days by exhaustive search.
- Being replaced by the Advanced Encryption Standard (AES): 128/196/256-bit keys, no significant attacks known.

6 Variants of DES

6.1 DES-X

Whitening: add two 64-bit values to key, and XOR these values before and after the core DES encryption. Cheap way to increase the cost of both exhaustive search and smart attacks (e.g., consider its effect on the simple attacks described above).

6.2 2DES, 3DES

- $\mathrm{2DES}_{K_I,K_{II}}(p) = \mathrm{DES}_{K_{II}}(\mathrm{DES}_{K_I}(p))$
- $\mathrm{3DES}_{K_I,K_{II},K_{III}}(p) = \mathrm{DES}_{K_{III}}(\mathrm{DES}^{-1}_{K_{II}}((\mathrm{DES}_{K_I}(p)))$
  The middle is decryption, for backward compatibility: $\mathrm{3DES}_{K,K,K}(p) = \mathrm{DES}_K(p)$.
  Sometimes used with just two keys: $K_I = K_{III}$.

Exercise 3. Show a "meet-in-the-middle" attack on 2DES, using 2^{56} memory (measured in blocks) and $\approx 2^{56}$ time (measured in DES operations).

- Is DES a group? That is, is the permutation defined by the composition of two DES encryptions always equivalent to the permutation defined by some other DES key? If so, then 2DES and 3DES don't buy any security. Fortunately, this isn't the case: there are just 2^{56} DES encryptions, by the order of the the permutation group generated by the DES encryptions is at least 10^{2499}.

1. Best theoretical attack on 3-key 3DES has complexity 2^{108}.

7 Modes of operation

Turn a block cipher into a stream cipher by adding memory. Note that the latency remains high (full block). See the bibliographic references on the course homepage for diagrams of the following.

- ECB: identical plaintext blocks -> identical ciphertext blocks. This leaks information, and causes malleability (i.e., an attacker can modify a ciphertext into another meaningful ciphertext).

- CBC: IV transmitted in plain (recall the Enigma message key). Equal plaintext blocks are encrypted to different ciphertext blocks. Blocks are also encrypted differently in different encrypted streams, if the IV is chosen randomly. Small error propagation (one block).

- OFB: No error propagation. Offline/online: we can prepare a "mask" stream of in advance, and then XOR it with the plaintext to get the ciphertext — this allows low latency during transmission. The IV must be chosen randomly for each message, otherwise the XOR of ciphertexts equals the XOR of the corresponding plaintexts.

- CFB: We can compute one block in advance to get low latency (as in OFB), but not more than one block.