1082 作業八

繳交日期 109/06/12(五) 13:10

1. Consider using CBC mode of encryption in the following way: the IV is treated as a key, and is assumed to be known to both Alice and Bob, but no actual encryption function is used. (That is, $E_K(x) = x$ for all K and all x.) We will investigate whether this yields any security.
   a. Show a known plaintext total break attack (i.e. one that yields IV) against this kind of cryptosystem.
   b. Discuss ciphertext-only attacks, both in the case that only one block is given and in the case that ℓ blocks are given for some $\ell > 1$
2. For a string of bits S, let $\overline{S}$ denote the complementary string obtained by changing all the 1's to 0's and all the 0's to 1's (equivalently, $S = \overline{S} \oplus 111111\ldots111$). Show that if the DES key K encrypts P to C, then $\overline{K}$ encrypts $\overline{P}$ to $\overline{C}$.
3. Before AES was developed, it was suggested to increase the security of DES with the product cipher DES × DES. This product cipher uses two 56-bit keys. Consider known-plaintext attacks on product ciphers. In general, suppose that we take the product of any cipher S = ($\mathcal{P}$, $\mathcal{P}$, $\mathcal{K}$, $\mathcal{E}$, $\mathcal{D}$) with itself. Further, suppose that $\mathcal{K} = \{0,1\}^n$ and $\mathcal{P} = \{0,1\}^m$. Now assume we have several plaintext-ciphertext pairs for the product cipher S^2, say $(x_1, y_1), \ldots, (x_\ell, y_\ell)$, all of which are obtained using the same unknown key, (K_1, K_2).
   a. Prove that $E_{K_1}(x_i) = D_{K_2}(y_i)$ for all i, $1 \le i \le \ell$. Give a heuristic argument that the expected number of keys (K_1, K_2) such that $E_{k_1}(x_i) = D_{K_2}(y_i)$ for all i, $1 \le i \le \ell$, is roughly $2^{2n-\ell m}$.
   b. Assume that $\ell \ge 2n/m$. A time-memory trade-off can be used to compute the unknown key (K_1, K_2). We compute two lists, each containing 2^n items, where each item contains an ℓ-tuple of elements of $\mathcal{P}$ as well as an element of $\mathcal{K}$. If the two lists are sorted, then a common ℓ-tuple can be identified by means of a linear search through each of the two lists. Show that this algorithm requires $2^{n+m+1}\ell + 2^{2n+1}$ bits of memory and $\ell\, 2^{n+1}$ encryptions and/or decryptions.
   c. Show that the memory requirement of the attack can be reduced by a factor of 2^t if the total number of encryptions is increased by a factor of 2^t. (Hint: Break the problem up into 2^{2t} subcases, each of which is specified by simultaneously fixing t bits of K_1 and t bits of K_2)

Hint: in 3.b, the lists are constructed as shown in the following figure