CHAPTER 14

Still Other Block Cipher

RC5 (Rivest Cipher)

- RC5 is a block cipher with a variety of parameters: block size, key size, and number of rounds.
- It was invented by Ron Rivest and analyzed by RSA laboratories.
- There are three operations: XOR, addition and rotations.
- RC5 is a variable length block, but we will focus on a 64-bit data block.
- Encryption uses 2r+2 key dependent 32-bit words – S_0, S_1, S_2,…, S_{2r+1}; where r is the number of rounds.
- To encrypt, first divide the plaintext block into two 32-bit words: A and B.

RC5 Continue…

- Then encryption is as follows:

$A = A + S_0$

$B = B + S_1$

For i = 1 to r:

$A = ((A \oplus B) <<< B) + S_{2i}$ <<< is left circular shift

$B = ((B \oplus A) <<< A) + S_{2i+1}$

Decryption is just as easy. Divide the Ciphertext block into two words, A and B and then

For i = r down to 1:

$B = ((B - S_{2i+1}) >>> A) \oplus A$

$A = ((A - S_{2i}) >>> B) \oplus B$

$B = B - S_1$

$A = A - S_0$

RC5 Continue…

- First step of key Expansion:
  - First copy the bytes of the key into an array, L, of c 32-bit words, padding the final word with zero if necessary.

- Second step of Key Expansion:
  - Then initialize an array S, using linear congruential generator mod 2^{32}.

$S_0 = P$

For i = 1 to 2(r+1)-1:

$S_i = (S_{i-1}+Q) \bmod 2^{32}$.

Where P = 0xb7e15163 and Q = 0x9e3779b9 are constant based on the binary representation of e and phi.

RC5 Continue…

- Third step of Key Expansion: (mix L into S)

  i=j=0

  A=B=0

  do 3n times (where n is the maximum of 2(r+1) and c):

  $A=S_i=(S_i+A+B)<<<3$

  $B=L_j=(L_j+A+B)<<<(A+B)$

  i=(i+1) mod 2(r+1)

  j=(j+1) mod c

We just defined RC5 with a 32-bit word size and 64-bit block; the same algorithm can also be used as a 64-bit word size and 128-bit block size. For w=64, P=0xb7e151628aed2a6b and Q=0x9e3779b97f4a7c15.

Rivest designates particular implementations of RC5 as RC5-w/r/b, where w is word size, r is round number and b is length of the key in bytes.