Information Systems Security
Series 4 - Correction

October 27th, 2021

Exercice 1 : Linear encryption

- The idea is to allow any ciphertext to be built with XORs of our 128 chosen ciphertexts. The simplest way to do that is to choose 128 ciphertexts where each one contains only one bit with value 1, each time at a different position, we'll note them $c_1, c_2, ..., c_{128}$ (c_i has only the i-th bit at value 1, and all other bits at value 0).
  We can now build any cipher $c = EL(m)$ as some XORs of our chosen ciphertexts (the ones where c has bits of value 1). And we know the decryption for these 128 chosen ciphertexts. We can note c as the XOR of a subset of the 128 chosen ciphertexts :

  $$c = c_{i_1} \oplus c_{i_2} \oplus ... \oplus c_{i_n} \ , \ c_{i_j} \in \{c_1, c_2, ..., c_{128}\} \ , \ i_j \in \{1, 2, ..., 128\}$$

  Here, the c_{i_j} are the subset of the 128 chosen ciphertexts needed to build c. Then we have :

  $$c = c_{i_1} \oplus c_{i_2} \oplus ... \oplus c_{i_n} = EL(k, m_{i_1}) \oplus EL(k, m_{i_2}) \oplus ... \oplus EL(k, m_{i_n}) = EL(k, m_{i_1} \oplus m_{i_2} \oplus ... \oplus m_{i_n})$$

  And we know these m_{i_j} since they are the decryptions of some of the 128 chosen ciphertexts, which gives us a very simple way to find the message :

  $$DL(c) = m = m_{i_1} \oplus m_{i_2} \oplus ... \oplus m_{i_n}$$

  We are now able to decipher anything without the key.
- Then it's obviously a very bad idea to have a linear encryption system.

Exercice 2 : Encryption Functions

To use an encryption function, we need to be able to decrypt it, which means the encryption function needs to be invertible.
(Reminder : For all function except the first one, B_i is included between 0 and 15 (as it is one hexadecimal digit), and so there's no two B_i that are equal mod 16 (if it wasn't the case, all these functions would obviously be impossible to invert).

1. $E = B \oplus K$ is usable, as XOR is invertible (and is its own inverse).
2. $E_i = (B_i + K_i) \mod 16$ is usable, as addition is invertible modulo 16.
3. $E_i = (B_i - 2 * K_i) \mod 16$ is usable. Multiplying the key by a constant does not change the fact that B - K is invertible.
4. $E_i = (2 * B_i - K_i) \mod 16$ is not usable. On the plaintext, it has some consequence, as 2 does not have a multiplicative inverse modulo 16. Then, we have some cases where two plaintexts are encrypted as one same cipher, and thus we can't decipher it : for example, $B_1 = 0$ and $B_1 = 8$ will both give $E_1 = (16 - K_1)$.
5. $E_i = (B_i * K_i) \mod 16$ is not usable either, as for some keys, we have the same problem as the previous function (for K_i=2 we have almost the same case).
6. $E_i = (7*B_i+K_i) \mod 16$ is usable : 7 has a multiplicative inverse modulo 16, and the function is then bijective (each B_i from 0 to 15 gives a different C_i).
7. $E_i = (4 * B_i + K_i) \mod 16$ is not usable, for the same reason that $2 * B_i$: for example, $B_i = 1$ and $B_i = 5$ will give the same cipher.
8. $E_1 = (3 * B_1 + K_2) \mod 16$, $E_2 = (11 * B_2 - K_1) \mod 16$ is usable, for the same reason as $7*B_i$: both 3 and 11 have multiplicative inverses (each other, as $3 * 11 = 33 = 1 \mod 16$).

Exercice 3 : ECB

- $C_1 = P_1 \oplus K = (A7)_{16} \oplus (AB)_{16} = (0C)_{16}$
  $C_2 = P_2 \oplus K = (41)_{16} \oplus (AB)_{16} = (EA)_{16}$
  $C_3 = P_3 \oplus K = (BA)_{16} \oplus (AB)_{16} = (11)_{16}$

  The ciphertext is C = $(0CEA11)_{16}$.

- $C_1 = (7*A+A \mod 16, 7*7+B \mod 16)_{16} = (80 \mod 16, 60 \mod 16)_{16} = (0C)_{16}$
  $C_2 = (7*4+A \mod 16, 7*1+B \mod 16)_{16} = (38 \mod 16, 18 \mod 16)_{16} = (62)_{16}$
  $C_2 = (7*B+A \mod 16, 7*A+B \mod 16)_{16} = (87 \mod 16, 81 \mod 16)_{16} =$

$(71)_{16}$

The ciphertext is C = $(0C6271)_{16}$.

Exercice 4 : CBC

- $C_1 = (P_1 \oplus IV) \oplus K = ((A7)_{16} \oplus (AD)_{16}) \oplus (AB)_{16} = (0A)_{16} \oplus (AB)_{16} = (A1)_{16}$
  $C_2 = (P_2 \oplus C_1) \oplus K = ((41)_{16} \oplus (A1)_{16}) \oplus (AB)_{16} = (E0)_{16} \oplus (AB)_{16} = (4B)_{16}$
  $C_3 = (P_3 \oplus IV) \oplus K = ((BA)_{16} \oplus (4B)_{16}) \oplus (AB)_{16} = (F1)_{16} \oplus (AB)_{16} = (5A)_{16}$

  The ciphertext is C = $(A14B5A)_{16}$.

- $C_1 = E_K(P_1 \oplus IV) = E_K((A7)_{16} \oplus (AD)_{16}) = E_K(0A) = (7 * 0 + A \mod 16, 7 * A + B \mod 16)_{16} = (10 \mod 16, 81 \mod 16)_{16} = (A1)_{16}$
  $C_2 = E_K(P_2 \oplus C_1) = E_K((41)_{16} \oplus (A1)_{16}) = E_K(E0) = (7 * E + A \mod 16, 7 * 0 + B \mod 16)_{16} = (108 \mod 16, 11 \mod 16)_{16} = (CB)_{16}$
  $C_3 = E_K(P_3 \oplus C_2) = E_K((BA)_{16} \oplus (CB)_{16}) = E_K(71) = (7 * 7 + A \mod 16, 7 * 1 + B \mod 16)_{16} = (59 \mod 16, 18 \mod 16)_{16} = (B2)_{16}$

  The ciphertext is C = $(A1CBB2)_{16}$.

Exercice 5 : CFB

- $C_1 = E_K(IV) \oplus P_1 = (7 * A + 7 \mod 16, 7 * A + 4 \mod 16)_{16} \oplus P_1 = (77 \mod 16, 74 \mod 16)_{16} \oplus P_1 = (DA)_{16} \oplus (24)_{16} = (FE)_{16}$
  $C_2 = E_K(C_1) \oplus P_2 = (7 * F + 7 \mod 16, 7 * E + 4 \mod 16)_{16} \oplus P_2 = (112 \mod 16, 102 \mod 16)_{16} \oplus P_2 = (06)_{16} \oplus (68)_{16} = (6E)_{16}$
  $C_3 = E_K(C_2) \oplus P_3 = (7 * 6 + 7 \mod 16, 7 * E + 4 \mod 16)_{16} \oplus P_3 = (49 \mod 16, 102 \mod 16)_{16} \oplus P_3 = (16)_{16} \oplus (AC)_{16} = (BA)_{16}$

  The ciphertext is C = $(FE6EBA)_{16}$.

- $P_1 = E_K(IV) \oplus C_1 = (7 * A + 7 \mod 16, 7 * A + 4 \mod 16)_{16} \oplus C_1 = (77 \mod 16, 74 \mod 16)_{16} \oplus C_1 = (DA)_{16} \oplus (12)_{16} = (C8)_{16}$
  $P_2 = E_K(C_1) \oplus C_2 = (7 * 1 + 7 \mod 16, 7 * 2 + 4 \mod 16)_{16} \oplus C_2 = (14 \mod 16, 18 \mod 16)_{16} \oplus C_2 = (E2)_{16} \oplus (34)_{16} = (D6)_{16}$
  $P_3 = E_K(C_2) \oplus C_3 = (7 * 3 + 7 \mod 16, 7 * 4 + 4 \mod 16)_{16} \oplus C_3 = (28 \mod 16, 32 \mod 16)_{16} \oplus C_3 = (C0)_{16} \oplus (56)_{16} = (96)_{16}$

  The original plaintext was P = $(C8D696)_{16}$.

Exercice 6 : OFB

- $C_1 = E_K(IV) \oplus P_1 = (11*A+7 \mod 16, 11*A+4 \mod 16)_{16} \oplus P_1 = (117 \mod 16, 114 \mod 16)_{16} \oplus P_1 = (52)_{16} \oplus (13)_{16} = (41)_{16}$
  $C_2 = E_K(E_K(IV)) \oplus P_2 = E_K((52)_{16}) \oplus P_2 = (11*5+7 \mod 16, 11*2+4 \mod 16)_{16} \oplus P_2 = (62 \mod 16, 26 \mod 16)_{16} \oplus P_2 = (EA)_{16} \oplus (57)_{16} = (BD)_{16}$
  $C_3 = E_K(E_K(E_K(IV))) \oplus P_3 = E_K((EA)_{16}) \oplus P_3 = (11*E+7 \mod 16, 11*A+4 \mod 16)_{16} \oplus P_3 = (161 \mod 16, 114 \mod 16)_{16} \oplus P_3 = (12)_{16} \oplus (9B)_{16} = (89)_{16}$

  The ciphertext is C = $(41BD89)_{16}$.

- $P_1 = E_K(IV) \oplus C_1 = (11*A+7 \mod 16, 11*A+4 \mod 16)_{16} \oplus C_1 = (117 \mod 16, 114 \mod 16)_{16} \oplus C_1 = (52)_{16} \oplus (12)_{16} = (40)_{16}$
  $P_2 = E_K(E_K(IV)) \oplus C_2 = E_K((52)_{16}) \oplus C_2 = (11*5+7 \mod 16, 11*2+4 \mod 16)_{16} \oplus C_2 = (62 \mod 16, 26 \mod 16)_{16} \oplus C_2 = (EA)_{16} \oplus (34)_{16} = (DE)_{16}$
  $P_3 = E_K(E_K(E_K(IV))) \oplus C_3 = E_K((EA)_{16}) \oplus C_3 = (11*E+7 \mod 16, 11*A+4 \mod 16)_{16} \oplus C_3 = (161 \mod 16, 114 \mod 16)_{16} \oplus C_3 = (12)_{16} \oplus (56)_{16} = (44)_{16}$

  The original plaintext was P = $(40DE44)_{16}$.