CSE 5473 — Network Security Autumn 2020

Assignment #1

Symmetric Cryptography *Due September 23rd, 11:59PM*

1 Secret Key Cryptography - DES [30 pts]

Answer:

1. The result is `37F32E892018D7ED`.
2. `0000000000000000` and `FFFFFFFFFFFFFFFF` are weak keys because their per-round keys are `0000000000000000` and `3f3f3f3f3f3f3f3f`, respectively.
3. To try all the 128 bit keys: $\frac{2^{128}}{10^6 \times 10^{12} \times 3600 \times 24 \times 365} = 1.08 \times 10^{13}$ years.

2 Encrypting Large Messages [40 pts]

Answer:

1. ECB: 1;
   CBC: 2;
   OFB: 1;
   CFB: because y_i is shifted in the IV_i, so the number of plaintext blocks that will be decrypted incorrectly is $1 + \frac{64}{k}$ (k is the block size). So, if k is 64 bits, 2 blocks will be garbled; if k is 8 bits, 9 blocks will be garbled. Refer to page 102-103 of the book for details.
2. With a weak DES key k, $E(x,k) = D(x,k)$, then $E(E(x,k),k) = D(E(x,k),k) = x$. Also, OFB has a block size of 64, so the current pad is encrypted (in whole) to generate the next pad. Therefore, the one-time pads are: $k\{IV\}, IV, k\{IV\}, IV, ...$
3. Yes, Name the pad sequence as $p_1 = k\{IV\}, p_2, ... , p_i, ... , p_j$, assume p_i is the first repeated pad (by p_j) and $1 < i < j$. Then, $p_{i-1} = D(p_i)$ and $p_{k-1} = D(p_k)$. Therefore, $p_{i-1} = p_{k-1}$. This contradicts with the assumption that p_i is the first repeated pad. This process can be repeated until there does not exist p_{i-1}. Only $i = 1$ does not has a precedent. So, p_1 must be the first repeated key.
4. In this question, we are dealing with message integrity check. Therefore, the message itself is in plaintext, with CBC residue appended to protect the message integrity. If you assume CBC is used for both privacy and integrity, you *need* to also assume that two different keys are used, one for privacy (encryption) and one for integrity. Moreover, the question says "the only constraint...". As such, you can make many assumptions (yes, include knowing the secret key).

   In this reference answer, I assume we already know the key and the plaintext message (IV is not used to compute CBC residue). The goal is to insert a garbage block somewhere in the message so the new message will have the specified CBC residue. We can construct the message in the following steps:

a. write down the message in the plaintext blocks and leave one block blank (to be used as the garbage block). Assume the garbage block is the ith block, so we need to compute (m_i).

b. using the key and previous message blocks, we can get c_{i-1} by computing forward from the first block: $c_{i-1} = E((c_{i-2} \oplus m_{i-1}), k)$

c. using the key, the residue and message blocks after m_i, we can also get c_i by computing backward from the CBC residue: $c_i = m_{i+1} \oplus D(c_{i+1}, k)$

d. Assign the garbage block: $m_i = c_{i-1} \oplus D(c_i, k)$

5. a. Yes, this scheme is reversible. To decrypt the message: $m_1 = D(c_1 \oplus IV, k)$, $m_2 = D(c_2 \oplus m_1, k)$, $m_3 = D(c_3 \oplus m_2, k)$...

   b. There are several security implications:

   - It is not self-synchronizing. Modifying, deleting or rearranging one block will garble the current block and all the blocks after the current one. Moreover, the IV only affects the first message block.
   - Since the plaintext block is computed by applying the decryption function last, the attacker can not predictably change the plaintext by modifying the cphertext without knowing the key. In CBC, this is doable because $m_i = c_{i-1} \oplus D(c_i, k)$. Changing c_{i-1} will garble m_{i-1}, but predictably flip bits in m_i.
   - Attackers knowing plaintext and ciphertext can rearrange the ciphertext with few limitations. This is because he can compute $E(m_i, k)$ for any message block without the key: $E(m_i, k) = m_{i-1} \oplus c_i$. With $E(m_i, k)$, he can rearrange ciphertext without garbling the message. For example, given $m_1|m_2|m_3$, the attacker can rearrange it into $m_3|m_2|m_1$ by sending the following ciphertext: $IV \oplus E(m_3, k)|m_3 \oplus E(m_2, k)|m_2 \oplus E(m_1, k)$. If IV is unknown to him, he will be forced to use m_1 as the first block (the only limitation).

3 Multiple Encryption DES [30 pts]

Answer:

1. Yes. The key to answer this question is to prove that using a second and third <m, c>pairs will significantly reduce the probability that $E(m_i, k_1) = E(c_i, k_2)$. The same reasoning applies to this variant as well except when $k_1 = k_2$. Though, we can safely assume $k_1 \neq k_2$ because it is obviously an unsafe use of ED: no work is required to reveal the plaintext, the ciphertext is always the same as the plaintext.

2. With triple DES (EDE), we can either meet between ED or DE. Assume the attack meets at the latter point. Then the meet-in-the-middle attack to break EDE is as

a. Make a table with 2^{112} entries (because two keys are used in this table, each has 2^{56} choices) where each entry consists of two DES keys K_1 and K_2 and the result $r = D(E(m_1, K_1), K_2)$. Sort the table by K_1, then by K_2 (Notice we sort the table by the keys. Sorting it by r would require a little more work to attack EDE than necessary.)

b. Make a second table with 2^{56} entries where each entry consists of a DES key K and the result $r = D(c_1, K)$. Sort the table by K.

c. To perform the attack, go through the entries in table 1 one by one, use K_1 to index into table 2 (to find $D(c_1, K_1)$), check whether two entries have the same result, i.e., $D(E(m_1, K_1), K_2) = D(c_1, K_1)$. If so, test the key pair K_1, K_2 with other <plaintext, ciphertext> pairs.

d. Extra practise: analyse the number of imposters and the probability to eliminate imposters by using extra pairs of <m_i, c_i>.

Notice, this attack is actually the same as the brutal force attack.

3. EDE with three keys is as secure as EDE with two keys. EDE with two keys can be attacked using brutal force with 2^{112} tries. Using meet-in-the-middle attack, EDE with three keys can be attacked with $2^{112} + 2^{56}$ tries (The beauty of meet-in-the-middle attack is turning the number of tries from multiplication to plus.)

   a. Build table 1 as in 2.a, but sort the table according to r.

   b. Build table 2 as in 2.b, but sort the table according to r.

   c. Like the meet-in-the-middle attack, go through these two tables to find entries with the same result ($2^{112} + 2^{56}$ steps). If so, verify these three keys with extra <m_i, c_i>pairs.

4. It takes twice the work for the attacker to brutal-force this scheme than the traditional DES. So it is (almost) not more secure than the traditional DES.

4 Breaking Monoaphabetic Cipher Using Frequence Analysis [30 points. There will be partial credit if you only partially solve it.]

Answer:

```
IHAVEBUTONELAMPBYWHICHMYFEETAREGUIDEDANDTHATIS
THELAMPOFEXPERIENCEIKNOWOFNOWAYOFJUDGINGOFTHE
FUTUREBUTBYTHEPASTANDJUDGINGBYTHEPASTIWISHTO
KNOWWHATTHEREHASBEENINTHECONDUCTOFTHEBRITISH
MINISTRYFORTHELASTTENYEARSTOJUSTIFYTHOSEHOPES
WITHWHICHGENTLEMENHAVEBEENPLEASEDTOSOLACE
THEMSELVESANDTHEHOUSEISITTHATINSIDIOUSSMILE
WITHWHICHOURPETITIONHASBEENLATELYRECEIVED
```

With spaces inserted:

```
I HAVE BUT ONE LAMP BY WHICH MY FEET ARE GUIDED
```

AND THAT IS THE LAMP OF EXPERIENCE I KNOW OF NO WAY OF JUDGING OF THE FUTURE BUT BY THE PAST AND JUDGING BY THE PAST I WISH TO KNOW WHAT THERE HAS BEEN IN THE CONDUCT OF THE BRITISH MINISTRY FOR THE LAST TEN YEARS TO JUSTIFY THOSE HOPES WITH WHICH GENTLEMEN HAVE BEEN PLEASED TO SOLACE THEMSELVES AND THE HOUSE IS IT THAT INSIDIOUS SMILE WITH WHICH OUR PETITION HAS BEEN LATELY RECEIVED