CSS322 – Quiz 5

Security and Cryptography, Semester 2, 2013

Prepared by Steven Gordon on 18 December 2013
css322y13s2q05, Steve/Courses/2013/s2/css322/assessment/quiz5.tex, r3040

Question 1 [3 marks]

Using block cipher *ABC* (the single version shown in the table), the plaintext [11010011 | 00101010 | 11010011 | 00101010] is encrypted using key [10 | 01 | 10 | 01] with CBC and IV [0110 | 0111 | 1110 | 1000] (encryption with CBC is shown in Figure 1 (left)). What is the ciphertext? [3 marks]

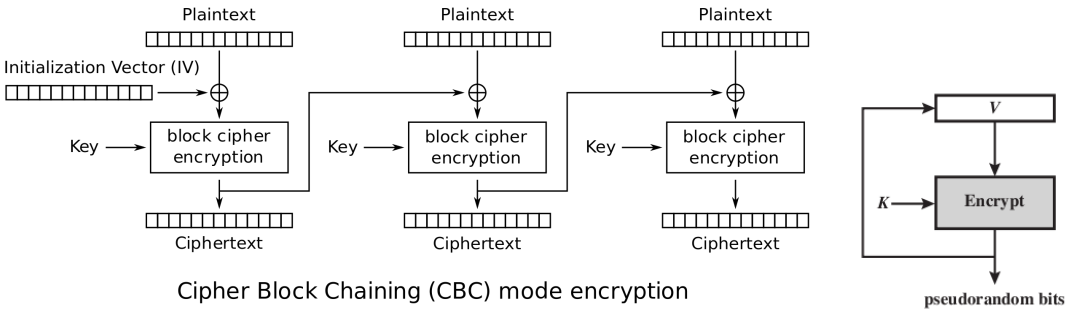

Figure 1: Left: CBC encryption; Right: Using block cipher for PRNG

Answer. *Split the plaintext into two 4-bit blocks then XOR the first block with the IV. The result is encrypted (lookup the ciphertext from the table), giving the first 4 bits of ciphertext. Then XOR the next 4-bits of plaintext with the previous ciphertext. The result is encrypted to give the last 4 bits of ciphertext.*

- *P: 1101 0011; IV=0110; K=10; C=1001 0000*
- *P: 0010 1010; IV=0111; K=01; C=1111 1111*
- *P: 1101 0011; IV=1110; K=10; C=1111 1010*
- *P: 0010 1010; IV=1000; K=01; C=0010 1011*

Question 2 [3 marks]

A block cipher can be used as a PRNG. One way is to select a key and initial value (together they are the seed), encrypt using the block cipher, and the output ciphertext is then fed as the next input to the block cipher (as shown in Figure 1 (right)). The ciphertext is the pseudorandom bits.

(a) What is the maximum possible period, in bits, of a pseudorandom stream generated when using an ideal [18 | 12 | 14 | 16]-bit block cipher? [1 mark]

Answer. *The period of PRNG is the number of output values produced before repeating. With a n-bit block cipher there are 2^n possible output blocks. Therefore when using that block cipher as a PRNG, there are 2^n possible different outputs. If the output is that same as a prior output, then the random stream has started to repeat. So with 2^n possible different outputs, each of n bits, the period of the PRNG in bits is $n \times 2^n$.*

(b) What is a disadvantage of using a real block cipher, like AES or Triple-DES, as a PRNG (as opposed to using a dedicated PRNG algorithm like Blum Blum Shub or LCG, or even a stream cipher like RC4)? [1 mark]

Answer. *Block ciphers are generally slower than dedicated PRNGs and stream ciphers.*

(c) You are given a sequence of 1 million bits. As one simple measure of "randomness" you would expect about half the bits to be 0's and half to be 1's. Explain another way you could measure the "randomness" of this sequence. [1 mark]

Answer. *One method is to divide the 1 million bits into subsequences (e.g. 500,000 bits, 100,000 bits, 1000 bits in length) and count the 0's and 1's in each subsequence. Again, they should be about the same. Or similarly count the number of sequences of pairs of bits (00, 01, 10, 11). There should be about the same number of occurrences of each pair (and extend to n-bit sequences). Another is to check if particular sequences repeat themselves. For example the sequence 01 should not repeat itself often like 01010101. There are many more advanced tests. Search on Wikipedia/Web for "randomness tests", "diehard tests", "Kolmogorov complexity".*

Question 3 [4 marks]

Consider a 4 bit block cipher, called *ABC*, that uses 2-bit keys. The ciphertext for all possible plaintexts and keys for cipher ABC are given below. To increase the strength of ABC against brute-force attack, I will apply the algorithm twice using a 4-bit key, K, which is two independent keys from ABC. The resulting cipher is *Double-ABC*. I have chosen a key and sent multiple ciphertexts to my friend. You are an attacker that has discovered two pairs of (plaintext, ciphertext): [(0111,1101) and (1101,0100) | (0000,0101) and (1111,0011) | (0111,1101) and (1101,0100) | (0000,0101) and (1111,0011)]. Use a meet-in-the-middle attack to determine the most likely key I used. Show the steps.

Answer. *Consider for the given pair (0111, 1101) and (1101, 1110).*
Using the pair (0111, 1101) apply a 2-bit brute force on the plaintext 0111 to get:
$K = 00, P = 0111, X_{1,1} = 1110$
$K = 01, P = 0111, X_{1,2} = 0001$
$K = 10, P = 0111, X_{1,3} = 0110$
$K = 11, P = 0111, X_{1,4} = 1111$
Now decrypt the ciphertext 1101 with all possible keys:

Plaintext	00	01	10	11		Plaintext	00	01	10	11
0000	0001	0101	1000	0111		1000	1000	1011	0101	1000
0001	1101	0111	1101	0101		1001	1100	0000	0010	0110
0010	0000	0110	0111	1010		1010	1010	0010	0000	0100
0011	0101	1101	1111	0011		1011	1011	1100	1001	1001
0100	0111	1000	1100	1101		1100	0110	0011	1010	1100
0101	1001	1111	1011	0001		1101	1111	1110	0100	0000
0110	0011	1001	0001	1011		1110	0100	0100	0011	0010
0111	1110	0001	0110	1111		1111	0010	1010	1110	1110

$K = 00, C = 1101, X_{2,1} = 0001$
$K = 01, C = 1101, X_{2,2} = 0011$
$K = 10, C = 1101, X_{2,3} = 0001$
$K = 11, C = 1101, X_{2,4} = 0100$
We note that there are two pairs of X that match:

(a) $X_{1,2} = X_{2,1}$ *giving a possible key 0100*

(b) $X_{1,2} = x_{2,3}$ *giving a possible key 0110*

So now try key 0100 with the next pair (1101,0100):
$P = 1101, K = 01, X = 1110, K = 00, C = 0100$
Since the key works for this pair we can assume this is the correct key. You could confirm by encrypting 1101 with the other key (0110) and you will see that the ciphertext 0100 is not *obtained. The correct key is 0100.*
Consider for the given pair (0000, 0101) and (1111, 0011).
Using the pair (0000, 0101) apply a 2-bit brute force on the plaintext 0000 to get:
$K = 00, P = 0000, X_{1,1} = 0001$
$K = 01, P = 0000, X_{1,2} = 0101$
$K = 10, P = 0000, X_{1,3} = 1000$
$K = 11, P = 0000, X_{1,4} = 0111$
Now decrypt the ciphertext 0101 with all possible keys:
$K = 00, C = 0101, X_{2,1} = 0011$
$K = 01, C = 0101, X_{2,2} = 0000$
$K = 10, C = 0101, X_{2,3} = 1000$
$K = 11, C = 0101, X_{2,4} = 0001$
We note that there are two pairs of X that match:

(a) $X_{1,1} = X_{2,4}$ *giving a possible key 0011*

(b) $X_{1,3} = x_{2,3}$ *giving a possible key 1010*

So now try key 0011 with the next pair (1111,0011):
$P = 1111, K = 00, X = 0010, K = 11, C = 0101$
The ciphertext doesn't match the expected value. So this is the wrong key. Lets try the next possible key 1010:
$P = 1111, K = 10, X = 1110, K = 10, C = 0011$
The ciphertext matches so the key 1010 is the correct key.