CSS322 – Quiz 2

Security and Cryptography, Semester 2, 2011

Prepared by Steven Gordon on 10 February 2012
CSS322Y11S2Q02, Steve/Courses/2011/S2/CSS322/Assessment/Quiz2.tex, r2148

Question 1 [5 marks]

Consider a 4 bit block cipher, called *ABC*, that uses 2-bit keys. The ciphertext for a selection of plaintext and keys for cipher ABC are given below.

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

To increase the strength of ABC against brute-force attack, you apply the algorithm twice using a 4-bit key, K, which is two independent keys from ABC. The resulting cipher is *Double-ABC*.

(a) If I choose the key 1100, what is the original plaintext for the ciphertext 0000? [2 marks]

Answer. *The 4-bit key consists of two 2-bit keys:* $K_1 = 11$ *and* $K_2 = 00$*. To decrypt you must use the two 2-bit keys in the opposite order, i.e.* K_2 *and then* K_1*. Decrypting 0000 with* $K_2 = 00$ *gives 0101 (look for the value 0000 in the column 00; the answer is the corresponding plaintext value). Now decrypting 0101 with* $K_1 = 11$ *gives 0001. Therefore the original plaintext was 0001.*

(b) I have chosen a new key and sent multiple ciphertexts to my friend. You are an attacker that has discovered a pair of (plaintext, ciphertext): (0111, 0001). Use a meet-in-the-middle attack to determine the most likely key I used. Show and explain the steps. [3 marks]

Answer. *Using the pair (0111, 0001) apply a 2-bit brute force on the plaintext 0111 to get:*

$K = 00, P = 0111, X_{1,1} = 0101$

$K = 01, P = 0111, X_{1,2} = 1101$

$K = 10, P = 0111, X_{1,3} = 1111$

$K = 11, P = 0111, X_{1,4} = 0011$

Now decrypt the ciphertext 0001 with all possible keys:

$K = 00, C = 0001, X_{2,1} = 0000$

$K = 01, C = 0001, X_{2,2} = 1111$

$K = 10, C = 0001, X_{2,3} = 1101$

$K = 11, C = 0001, X_{2,4} = 1001$

We note that there are two pairs of X that match:

i. $X_{1,2} = X_{2,3}$ *giving a possible key 0110*

ii. $X_{1,3} = x_{2,2}$ *giving a possible key 1001*

There is no way to know which key is correct (another plaintext, ciphertext pair could help). Either 0110 or 1001 can potentially be the correct key. This was a mistake in the quiz in that I didn't see the 2nd pair, thinking the only possible key was 0110.

Question 2 [4 marks]

(a) You select two prime numbers to use in RSA key generation to be: [19, 7 | 7, 23 | 13, 19 | 17, 13]. Calculate and fill in the values for the two keys generated if e is the smallest valid value chosen which is greater than [5 | 10 | 7 | 8]. [3 marks]

PU = (_____ , _____) and PR = (_____ , _____)

Answer. *The general solution is find* $n = p \times q$*, then find* $\phi(n) = (p-1) \times (q-1)$*. e must be relatively prime with* $\phi(n)$ *and greater than the value specified in the question. Then find d such that* $e \times d \bmod \phi(n) = 1$*. Finally the public key, PU, is* (e, n) *and the private key, PR, is* (d, n)*.*

i. $p = 19, q = 7, n = 133, \phi(133) = 108, e = 7, d = 31; PU = (7, 133), PR = (31, 133)$

ii. $p = 7, q = 23, n = 161, \phi(161) = 132, e = 13, d = 61; PU = (13, 161), PR = (61, 161)$

iii. $p = 13, q = 19, n = 247, \phi(247) = 216, e = 11, d = 59; PU = (11, 247), PR = (59, 247)$

iv. $p = 13, q = 17, n = 221, \phi(221) = 192, e = 11, d = 35; PU = (11, 221), PR = (35, 221)$

(b) Write an equation that represents the decryption of the ciphertext [23 | 49 | 17 | 24] that was confidentially sent using the keys in part (a). You may use the actual values (e.g. 3), or simply variables (e.g. e) in your equation. You don't have to calculate the answer, just write the equation. [1 mark]

Answer. $M = C^d \bmod n$

Question 3 [1 marks]

Which of the following cannot be used as a PRNG?

(a) ANSI X9.17

(b) Blum Blum Shub

(c) 3DES

(d) RC4

(e) LCG

(f) None of the above

Answer. *None of the above. All are either pseudorandom number generators or can be used as a PRNG.*