Name: Student ID:

Information Security, Fall 2016

Homework #2: Part 1 Symmetric Ciphers, Part 2 Asymmetric Ciphers

Graded out of 10 points. Due: 11/3 (Thursday)(End of the class)

1. How many bytes in **State** are affected by ShiftRows?

Ans: 12 bytes.

2. Given the plaintext {000102030405060708090A0B0C0D0E0F} and the key {01010101010101010101010101010101}:

a. Show the original contents of **State**, displayed as a 4 * 4 matrix.

b. Show the value of **State** after initial AddRoundKey.

c. Show the value of **State** after SubBytes.

d. Show the value of **State** after ShiftRows.

e. Show the value of **State** after MixColumns. [Just report the diagonal elements here, i.e. $S_{0,0}$, $S_{1,1}$, $S_{2,2}$, $S_{3,3}$]

Ans: (b)(ex. 00=0000 0000, XOR with the key 01=0000 0001. So the result will be 0000 0001=01)

(c)(need to check table 5.2 for AES S-Box. So 01 in the S-Box is 7C)

00	04	08	0C
01	05	09	0D
02	06	0A	0E
03	07	0B	0F

a

01	05	09	0D
00	04	08	0C
03	07	0B	0F
02	06	0A	0E

b

7C	6B	01	D7
63	F2	30	FE
7B	C5	2B	76
77	6F	67	AB

c

7C	6B	01	D7
F2	30	FE	63

75			
	E6		

2B	76	7B	C5
AB	77	6F	67

d

		B8	
			0A

e

3. What is a meet-in-the-middle attack?

Ans: This is an attack used against a double encryption algorithm and requires a known (plaintext, ciphertext) pair. In essence, the plaintext is encrypted to produce an intermediate value in the double encryption, and the ciphertext is decrypted to produce an intermediation value in the double encryption. Table lookup techniques can be used in such a way to dramatically improve on a brute-force try of all pairs of keys.

4. If a bit error occurs in the transmission of a ciphertext character in 8-bit CFB mode, how far does the error propagate?

Ans: Only the plaintext unit corresponding to the ciphertext character is affected. In CFB method, the bit errors in transmission do not propagate. For example, if a bit error occurs in C1, only the recovered value of P1 is affected; subsequent plaintext units are not corrupted.

5. What is the difference between a one-time pad and a stream cipher?

Ans: One-time pad uses a genuine random number stream, whereas a stream cipher uses a pseudorandom number stream.

6. Alice and Bob agree to communicate privately via email using a scheme based on RC4, but they want to avoid using a new secret key for each transmission. Alice and Bob privately agree on a 128-bit key k. To encrypt a message m, consisting of a string of bits, the following procedure is used.

1. Choose a random 80-bit value v

2. Generate the ciphertext $c = RC4(v \,||\, k) \oplus m$

3. Send the bit string $(v \,||\, c)$

Suppose Alice uses this procedure to send a message m to Bob. Describe how Bob can recover the message m from (v || c) using k.

Ans: By taking the first 80 bits of $v \,||\, c$, we obtain the initialization vector, v. Since v, c, k are known, the message can be recovered (i.e., decrypted) by computing RC4($v \,||\, k$) $\oplus$ c.

Bob known v, c, k.

Compute RC4(v||k)

Compute RC4(v||k) $\oplus$ c = m.

Therefore, Bob can recover m.

7. What is a prime number?

Ans: An integer $p > 1$ is a prime number if and only if its only divisors are ± 1 and $\pm p$.

8. Use **Fermat's theorem** to find a number x between 0 and 28 with x^{85} congruent to *6 modulo 29*. (You should not need to use any brute-force searching. Must answering with Fermat's theorem)

Ans. 6

$X^{85} \equiv 6 \pmod{29}$.

Using Fermat's theorem, $a^{p-1} \equiv 1 \pmod{p}$, $a^{28} \equiv 1 \pmod{29}$.

Therefore, $x^{85} = (x^{28})^3 \times x \equiv 6 \pmod{29}$, $1 \times x = 6$, so x=6.

9. What requirements must a public-key cryptosystems fulfill to be a secure algorithm?

Ans:
1. It is computationally easy for a party B to generate a pair (public key PU_b, private key PR_b).
2. It is computationally easy for a sender A, knowing the public key and the message to be encrypted, M, to generate the corresponding ciphertext:

$$C = E(PU_b, M)$$

3. It is computationally easy for the receiver B to decrypt the resulting ciphertext using the private key to recover the original message:

$$M = D(PR_b, C) = D(PR_b, E(PU_b, M))$$

4. It is computationally infeasible for an opponent, knowing the public key, PU_b, to determine the private key, PR_b.

5. It is computationally infeasible for an opponent, knowing the public key, PU_b, and a ciphertext, C, to recover the original message, M.

10. In a public-key cryptsystem using RSA, given the ciphertext $C = 61$ and the public key $e = 11$, $n = 91$, find the plaintext M.

Ans: 3