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?

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. $S_{0,0}$, $S_{1,1}$, $S_{2,2}$, $S_{3,3}$]

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

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

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

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*.

7. What is a prime number?

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)

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

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.*