Name: Student ID:

Information Security, Fall 2016

Homework #1: Part 1 Symmetric Cipher

Graded out of 10 points. Due: 10/20 (Thursday)

1.List and briefly define the three key objectives of computer security.

2. List the parameters used to characterize cryptographic systems.

3. A generalization of the Caesar cipher, known as the affine Caesar cipher, has the following form: For each plaintext letter *p*, substitute the ciphertext letter *C*:

$C = E([a, b], p) = (ap + b) \bmod 26$

A basic requirement of any encryption algorithm is that it be one-to-one. That is, if $p \neq q$, then $E(k, p) \neq E(k, q)$. Otherwise, decryption is impossible, because more than one plaintext character maps into the same ciphertext character. The value of *b* in above equation shifts the relationship between plaintext letters and ciphertext letters to the left or right uniformly, so that if the mapping is one-to-one it remains one-to-one.

a. Suppose $a = 4$ and $b = 6$, compute $C_1 = E([a, b], 0)$ and $C_2 = E([a, b], 13)$.

b. Is it possible to decrypt the cipher in part (a)? Explain why or why not.

c. Is the affine Caesar cipher one-to-one for all values of a? Justify.

4. This problem explores the use of a one-time pad version of the Vigenère cipher. In this scheme, the key is a stream of random numbers between 0 and 26. For example, if the key is 3 19 5 . . . , then the first letter of plaintext is encrypted with a shift of 3 letters, the second with a shift of 19 letters, the third with a shift of 5 letters, and so on.

a. Encrypt the plaintext 'cryptography' with the key stream

10 22 5 4 1 0 2 9 18 16 16 0

b. Using the ciphertext produced in part (a), find a key so that the cipher text decrypts to the plaintext 'applications'.

5. The 32-bit swap after the sixteenth iteration of the DES algorithm is needed to make the encryption process invertible by simply running the ciphertext back through the algorithm with the key order reversed. However, it still may not be entirely clear why the 32-bit swap is needed. To demonstrate why, solve the following exercises. First, some notation:

$A||B$ = the concatenation of the bit strings A and B

$T_i(R||L)$ = the transformation defined by the *i*th iteration of the encryption algorithm for $1 \leq I \leq 16$

$TD_i(R||L)$ = the transformation defined by the *i*th iteration of the encryption algorithm for $1 \leq I \leq 16$

$T_{17}(R||L) = L||R$, where this transformation occurs after the sixteenth iteration of the encryption algorithm

a. Show that the composition $TD_1(IP(IP^{-1}(T_{17}(T_{16}(L_{15}||R_{15})))))$ is equivalent to the transformation that interchanges the 32-bit halves, L_{15} and R_{15}.That is, show that $TD_1(IP(IP^{-1}(T_{17}(T_{16}(L_{15}||R_{15}))))) = R_{15}||L_{15}$

b. Now suppose that we did away with the final 32-bit swap in the encryption algorithm. Then we would want the following equality to hold: $TD_1(IP(IP^{-1}(T_{16}(L_{15}\ ||R_{15})))) = L_{15}\ ||R_{15}$
Does it? Justify.

6. Does the set of residue classes (mod3) form a group

a. with respect to modular addition?

b. with respect to modular multiplication?

Justify with tables and axioms.

7. For each of the following equations, find an integer that satisfies the equation.

a. 10x ≡ 5 (mod 9)

b. 3x ≡ 2 (mod 8)

c. 3x ≡ 3(mod 4)

8. Develop a set of tables similar to the following for GF(5).

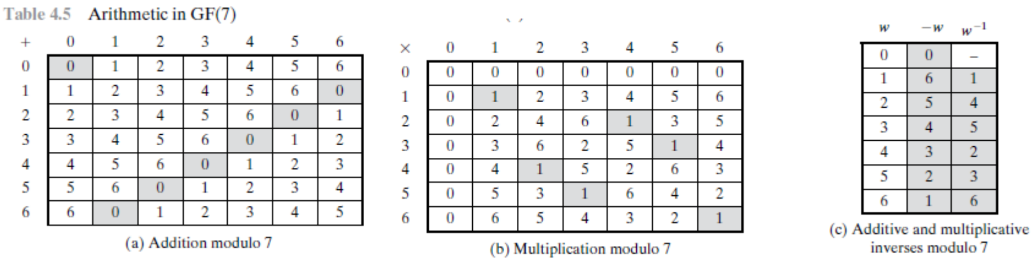

Table 4.5 Arithmetic in GF(7)

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

(a) Addition modulo 7

×	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

(b) Multiplication modulo 7

w	$-w$	w^{-1}
0	0	–
1	6	1
2	5	4
3	4	5
4	3	2
5	2	3
6	1	6

(c) Additive and multiplicative inverses modulo 7

9. Determine the gcd of the following pairs of polynomials: X^3+x+1 and x^2+x+1 over GF(2).

10. Determine the multiplicative inverse of x^3+x+1 in GF(2^4) with $m(x) = x^4+x+1$.