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.

Ans: Confidentiality, Integrity and Availability (CIA) are the three key objectives of computer security. Confidentiality preserves authorized restrictions on information access and protects personal privacy and proprietary information. Integrity guards against improper information modification or destruction, and also ensures information non-repudiation and authenticity. Availability assures that systems work promptly and service is not denied to authorized users.

2. List the parameters used to characterize cryptographic systems.

Ans:Following parameters are used to characterize the cryptographic systems:

a. The type of operations used for transforming plaintext to ciphertext.
b. The number of keys used and
c. The way in which the plaintext is processed.

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) mod 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.

Ans: a. C1 = E([a, b], 0) = (4 × 0) + 6 mod 26 = 6 and

C2 = E([a, b], 13) = (4 × 13) + 6 mod 26 = 58 mod 26 = 6.

b. No, it is not possible to decrypt the cipher obtained in part (a) because more than one plaintext character maps into the same ciphertext character.
c. Based on the cipher values obtained in part (a) where a = 4, it can be observed that the affine Caesar cipher is not one-to-one for all values of a.

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'.

Ans: a.

c	r	y	p	t	o	g	r	a	p	h	y
2	17	24	15	19	14	6	17	0	15	7	24
10	22	5	4	1	0	2	9	18	16	16	0
12	**13**	**3**	**19**	**20**	**14**	**8**	**0**	**18**	**5**	**23**	**24**
M	**N**	**D**	**T**	**U**	**O**	**I**	**A**	**S**	**F**	**X**	**Y**

b.

a	p	p	l	i	c	a	t	i	o	n	s
0	15	15	11	8	2	0	19	8	14	13	18
12	**24**	**14**	**8**	**12**	**12**	**8**	**7**	**10**	**17**	**10**	**6**
12	13	3	19	20	14	8	0	18	5	23	24
M	N	D	T	U	O	I	A	S	F	X	Y

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 *$1 \le I \le 16$

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

***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.

Ans: **a.** Let us work this from the inside out.

$T_{16}(L_{15} \,||\, R_{15}) = L_{16} \,||\, R_{16}$

$T_{17}(L_{16} \,||\, R_{16}) = R_{16} \,||\, L_{16}$

$IP\,[IP^{-1}\,(R_{16} \,||\, L_{16})] = R_{16} \,||\, L_{16}$

$TD_1(R_{16} \,||\, L_{16}) = R_{15} \,||\, L_{15}$

b. $T_{16}(L_{15} \,||\, R_{15}) = L_{16} \,||\, R_{16}$

$IP\,[IP^{-1}\,(L_{16} \,||\, R_{16})] = L_{16} \,||\, R_{16}$

$TD_1(R_{16} \,||\, L_{16}) = R_{16} \,||\, L_{16} \oplus f(R_{16}, K_{16})$

$\neq L_{15} \,||\, R_{15}$

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.

Ans: Here are the addition and multiplication tables

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

×	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

a. Yes. The identity element is 0, and the inverses of 0, 1, 2 are respectively 0, 2, 1.
Explain with Axioms as following examples.

(A1) Closure: If a and b belong to S, then a+b is also in S. The sum of any two elements in the residue class is also in the class.

(A2) Associative: a+(b+c)=(a+b)+c for all a, b, c in S. The residue class is associative under addition, by observation.

(A3) Identity element: There is an element 0 in R such that a+0=0+a=a for all a in S. 0, 1, 2 are the additive identity elements for addition.

(A4) Inverse element: For each a in S there is an element –a in S such that a+(-a)=(-a+a)=0. The additive inverses of 0, 1, 2 are respectively 0, 2, 1.

(A5) Commutative: a+b=b+a for all a, b in S.

0, 1, 2 are commutative under addition, by observation.

b. No. The identity element is 1, but 0 has no inverse. Explain with 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)

Ans: **a.** 5 **b.** 6 **c.** 5 There are other correct answers.

8. Develop a set of tables similar to Table 4.5 for GF(5).

Ans:

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

w	$-w$	w^{-1}
0	0	—
1	4	1
2	3	3
3	2	2
4	1	4

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

Ans: 1

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

Ans: $x^2 + 1$