Suggested Solutions to Homework Assignment #1A

(prepared by Wei-Hsien Chang)

1. Exercise problems from [Stallings]:

1.1 **Confidentiality** - Only authorized personnel must be able to obtain information from the implanted unit. This is of high importance, since personal health information in the wrong hands can, in some cases, lead to severe health risks to the patient. In this case, confidentiality implies that a valid PIN is not easy to forge, nor is it possible to copy one from an authorized source.

Integrity - The information collected by the implanted unit must not be tampered with, and when data is requested from the unit, the retrieved data must match that which was collected by the implanted unit. This is of high importance, since incorrect information might lead to incorrect or untimely treatment, which can result in severe health risks to the patient.

Availability - Collected data must be retrievable at all times by an authorized party. The importance of this requirement depends on the type of information that is being collected. For example, availability is of high importance for heart rate monitors, while information regarding sleep patterns can be accessed less frequently without much loss of utility to the system.

2.1 **a.** No. A change in the value of b 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.

b. 0, 2, 4, 6, 8, 10, 12, 13, 14, 16, 18, 20, 22, 24. Any value of a larger than 25 is equivalent to a mod 26.

c. The values of a and 26 must have no common positive integer factor other than 1. This is equivalent to saying that a and 26 are relatively prime, or that the greatest common divisor of a and 26 is 1. To see this, first note that $E(a, p) = E(a, q)$ $(0 \leq p \leq q < 26)$ if and only if $a(p - q)$ is divisible by 26.
1. Suppose that a and 26 are relatively prime. Then, $a(p-q)$ is not divisible by 26, because there is no way to reduce the fraction $a/26$ and $(p - q)$ is less than 26.
2. Suppose that a and 26 have a common factor $k > 1$. Then $E(a, p) = E(a, q)$, if $q = p + m/k \neq p$.

2.12 **a.** $25! = 2^{84}$

b. Given any $5 * 5$ configuration, any of the four row rotations is equivalent, for a total of five equivalent configurations. For each of these five configurations, any of the four column rotations is equivalent. So each configuration in fact represents 25 equivalent configurations. Thus, the total number of unique keys is $25!/25 = 24!$

3.1 **b.** In theory, the key length could be $log_2(2^n)!$ bits. For example, assign each mapping a number, from 1 through $(2^n)!$ and maintain a table that shows the mapping for each such number. Then, the key would only require $log_2(2^n)!$ bits, but we would also require this huge table. A more straightforward way to define the key is to have the key consist of the ciphertext value for each plaintext block, listed in sequence for plaintext blocks 0 through $2^n - 1$. This is what is suggested by Table 3.1. In this case the key size is $n \times 2^n$ and the huge table is not required.

3.3 **a.** We need only determine the probability that for the remaining $N - t$ plaintexts P_i, we have $E[K, P_i] \neq E[K', P_i]$. But $E[K, P_i] = E[K', P_i]$ for all the remaining P_i with probability $1 - 1/(N - t)!$.

b. Without loss of generality we may assume the $E[K, P_i] = P_i$ since $EK(\bullet)$ is taken over all permutations. It then follows that we seek the probability that a permutation on $N - t$ objects has exactly t' fixed points, which would be the additional t' points of agreement between $E(K, \bullet)$ and $E(K', \bullet)$. But a permutation on $N - t$ objects with t' fixed points is equal to the number of ways t' out of $N - t$ objects can be fixed, while the remaining $N - t - t'$ are not fixed. Then

Pr(t' additional fixed points)

$= C_{t'}^{N-t} \times$ Pr(no fixed points in $N - t - t'$ objects)

$$= \frac{1}{t'!} \times \sum_{k=0}^{N-t-t'} \frac{(-1)^k}{k!}$$

We see that this reduces to the solution to part (a) when $t' = N - t$.

3.12

Round Number	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Bits Rotate	0	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

4.13

$1^{-1} = 1$ $\quad 1 \times 1 = 1 \bmod 13$

$2^{-1} = 7$ $\quad 2 \times 7 = 14 = 1 \bmod 13$

$3^{-1} = 9$ $\quad 3 \times 9 = 27 = 1 \bmod 13$

$4^{-1} = 10$ $\quad 4 \times 10 = 40 = 1 \bmod 13$

$5^{-1} = 8$ $\quad 5 \times 8 = 40 = 1 \bmod 13$

$6^{-1} = 11$ $\quad 6 \times 11 = 66 = 1 \bmod 13$

$7^{-1} = 2$ $\quad 7 \times 2 = 14 = 1 \bmod 13$

$8^{-1} = 5$ $\quad 8 \times 5 = 40 = 1 \bmod 13$

$9^{-1} = 3$ $\quad 9 \times 3 = 27 = 1 \bmod 13$

$10^{-1} = 4$ $\quad 10 \times 4 = 40 = 1 \bmod 13$

$11^{-1} = 6$ $\quad 11 \times 6 = 66 = 1 \bmod 13$

$12^{-1} = 12$ $\quad 12 \times 12 = 144 = 1 \bmod 13$

4.14 $1 \equiv 1 \pmod 9$; $10 \equiv 1 \pmod 9$; $10^2 \equiv 10(10) \equiv 1(1) \equiv 1 \pmod 9$; $10^{n-1} \equiv 1 \pmod 9$. Express N as $a_0 + a_1 10^1 + \ldots + a_{n-1} 10^{n-1}$. Then $N \equiv a_0 + a_1 + \ldots + a_{n-1} \pmod 9$.

4.19 **a.** In order to find the multiplicative inverse of 5678 mod 8765, gcd(8765, 5678) is calculated using the Extended Euclidean algorithm. The following table lists the stages of the algorithm:

i	r	q	x	y
-1	8765		1	0
0	5678		0	1
1	3087	1	1	-1
2	2591	1	-1	2
3	496	1	2	-3
4	111	5	-11	17
5	52	4	46	-71
6	7	2	-103	159
7	3	7	767	-1184
8	1	2	-1637	2527

Thus, the multiplicative inverse of 5678 mod 8765 is 2527.

c. In order to find the multiplicative inverse of 826 mod 2789, gcd(826, 2789) is calculated using the Extended Euclidean algorithm. The following table lists the stages of the algorithm:

i	r	q	x	y
-1	2789		1	0
0	826		0	1
1	311	3	1	-3
2	204	2	-2	7
3	107	1	3	-10
4	97	1	-5	17
5	10	1	8	-27
6	7	9	-77	260
7	3	1	85	-287
8	1	2	-247	834

Thus, the multiplicative inverse of 826 mod 2789 is 834.

4.26 Polynomial Arithmetic Modulo $(x^2 + 1)$:

		000	001	010	011
	$+$	0	1	x	$x+1$
000	0	0	1	x	$x+1$
001	1	1	0	$x+1$	x
010	x	x	$x+1$	0	1
011	$x+1$	$x+1$	x	1	0

		000	001	010	011
	$\times$	0	1	x	$x+1$
000	0	0	0	0	0
001	1	0	1	x	$x+1$
010	x	0	x	$x+1$	1
011	$x+1$	0	$x+1$	1	x

4.27 In order to find the multiplicative inverse of $x^5 + x^4 + x^2 + 1$ in GF(2^8) with $m(x) = x^8 + x^4 + x^3 + x + 1$, gcd$(x^8 + x^4 + x^3 + x + 1, x^5 + x^4 + x^2 + 1)$ is calculated using the

Extended Euclidean algorithm for polynomials. The following table lists the stages of the algorithm:

i	**r(x)**	**q(x)**	**v(x)**	**w(x)**
-1	$x^8 + x^4 + x^3 + x + 1$		1	0
0	$x^5 + x^4 + x^2 + 1$		0	1
1	$x^3 + x^2 + 1$	$x^3 + x^2 + x$	1	$x^3 + x^2 + x$
2	1	x^2	x^2	$x^5 + x^4 + x^3 + 1$

Thus, the multiplicative inverse of $x^5 + x^4 + x^2 + 1$ under the conditions of the question is $x^5 + x^4 + x^3 + 1$.

2. We have discussed in class a known plaintext attack on the Hill cipher. What are the criteria on the known plaintext-ciphertext pairs for the attack to succeed?
Please be as precise as possible and explain the reasons for such criteria. (10 points)

Solution. Take the 2-dimentional Hill Cipher as an example. Suppose we have got 2 plaintext-ciphertext pairs, $([P_{11}, P_{12}], [C_{11}, C_{12}])$ and $([P_{21}, P_{22}], [C_{21}, C_{22}])$. Let $\mathbf{P}$ be the plaintext matrix $\begin{bmatrix} p_{11} & p_{12} \\ p_{21} & p_{22} \end{bmatrix}$ and $\mathbf{C}$ the ciphertext matrix $\begin{bmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{bmatrix}$. According to the Hill Cipher, $\mathbf{PK} = \mathbf{C} \bmod 26$ for some key matrix $\mathbf{K}$. We may obtain $\mathbf{K}$ by multiplying each side with $\mathbf{P}^{-1}$ (if it exists), that is, $\mathbf{K} = \mathbf{P}^{-1}\mathbf{PK} = \mathbf{P}^{-1}\mathbf{C}$. For $\mathbf{P}^{-1}$ to exist, $\det(\mathbf{P})$ should not equal 0 (mod 26), i.e., $p_{11} \times p_{22} - p_{12} \times p_{21} \not\equiv 0 \pmod{26}$. □