Suggested Solutions to Homework Assignment #1A

1 Exercise problems from [Stallings 2011]:

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 $q = p + m/k \neq p$.

2.8 SPUTNIK

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 $n \times 2n$ 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 $t' = N - t$.

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 $N \equiv a_0 + a_1 + \ldots + a_{n-1} \pmod 9$.

4.16 **a.** We want to show that $m > 2r$. This is equivalent to $qn + r > 2r$, which is equivalent to $qn > r$. Since $n > r$, we must have $qn > r$.

b. If you study the pseudocode for Euclid's algorithm in the text, you can see that the relationship defined by Euclid's algorithm can be expressed as

$A_i = q_{i+1} A_{i+1} + A_{i+2}$

The relationship $A_{i+2} < A_i/2$ follows immediately from (a).

c. From (b), we see that $A_3 < 2^{-1} A_1$, that $A_5 < 2^{-2} A_3 < 2^{-2} A_1$, and in general that $A_{2j+1} < 2^{-j} A_1$ for all integers j such that $1 < 2j + 1 \leq k + 2$, where k is the number of steps in the algorithm. If k is odd, we take $j = (k+1)/2$ to obtain $N > (k+1)/2$, and if k is even, we take $j = k/2$ to obtain $N > k/2$. In either case $k < 2N$.

4.17 **a.** Euclid: gcd(2152, 764) = gcd(764, 624) = gcd(624, 140) = gcd(140, 64) = gcd(64, 12) = gcd(12, 4) = gcd(4, 0) = 4

Stein: A1 = 2152, B1 = 764, C1 = 1; A2 = 1076, B2 = 382, C2 = 2; A3 = 538, B3 = 191, C3 = 4; A4 = 269, B4 = 191, C4 = 4; A5 = 78, B5 = 191, C5 = 4; A5 = 39, B5 = 191,C5 = 4; A6 = 152, B6 = 39, C6 = 4; A7 = 76, B7 = 39, C7 = 4; A8 = 38, B8 = 39, C8 = 4; A9 = 19, B9 = 39, C9 = 4; A10 = 20, B10 = 19, C10 = 4; A11 = 10, B11 = 19, C11 = 4; A12 = 5, B12 = 19, C12 = 4; A13 = 14, B13 = 5, C13 = 4; A14 = 7, B14 = 5, C14 = 4;A15 = 2, B15 = 5, C15 = 4; A16 = 1, B16 = 5, C16 = 4; A17 = 4, B17 = 1, C17 = 4;A18 = 2, B18 = 1, C18 = 4; A19 = 1, B19 = 1, C19 = 4; gcd(2152, 764) = $1 \times 4 = 4$

b. Euclid's algorithm requires a "long division" at each step whereas the Stein algorithm only requires division by 2, which is a simple operation in binary arithmetic.

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.

b. gcd(20736, 5994) = 162 ≠ 1, so there is no multiplicative inverse.

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	1	$x+1$
011	$x+1$	0	$x+1$	$x+1$	0

4.27 1

2. The $n \times n$ Hill cipher (encrypting n successive plaintext letters at a time) can be represented as $C_{1\times n} = P_{1\times n}K_{n\times n}$. Here we have written $P_{1\times n}$ and $C_{1\times n}$ to signify that the plaintext and the ciphertext are row vectors of n letters, while the key is an $n \times n$ matrix. Given n plaintext-ciphertext pairs, we can form the equation $C_{n\times n} = P_{n\times n}K_{n\times n}$. If the inverse P^{-1} of P exists, we multiply both sides with P^{-1} to get $P^{-1}C = P^{-1}PK = K$ and hence the key K. For P^{-1} to exist, P must have a nonzero determinant so that it is invertible. So, the criteria on the known plaintext-ciphertext pairs for the attack to succeed are (1) we have at least n plaintext-ciphertext pairs and (2) the plaintext in n of these pairs form a matrix with nonzero determinant.