

## 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  $a \pmod{26}$ .
- 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  $n \times 2^n$  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

$$\begin{aligned} & \Pr(t' \text{ additional fixed points}) \\ &= C_{t'}^{N-t} \times \Pr(\text{no fixed points in } N - t - t' \text{ objects}) \\ &= \frac{1}{t'!} \times \sum_{k=0}^{N-t-t'} \frac{(-1)^k}{k!} \end{aligned}$$

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

<b>3.12</b>	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**

$$\begin{aligned} 1^{-1} &= 1 & 1 \times 1 &= 1 \pmod{11} \\ 2^{-1} &= 6 & 2 \times 6 &= 12 = 1 \pmod{11} \\ 3^{-1} &= 4 & 3 \times 4 &= 12 = 1 \pmod{11} \\ 4^{-1} &= 3 & 4 \times 3 &= 12 = 1 \pmod{11} \\ 5^{-1} &= 9 & 5 \times 9 &= 45 = 1 \pmod{11} \\ 6^{-1} &= 2 & 6 \times 2 &= 12 = 1 \pmod{11} \\ 7^{-1} &= 8 & 7 \times 8 &= 56 = 1 \pmod{11} \\ 8^{-1} &= 7 & 8 \times 7 &= 56 = 1 \pmod{11} \\ 9^{-1} &= 5 & 9 \times 5 &= 45 = 1 \pmod{11} \\ 10^{-1} &= 10 & 10 \times 10 &= 100 = 1 \pmod{11} \end{aligned}$$

**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  $a_0 + a_1 10^1 + \dots + a_{n-1} 10^{n-1}$ . Then  $N \equiv a_0 + a_1 + \dots + a_{n-1} \pmod{9}$ .

**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.

**b.**  $\gcd(20736, 5994) = 162 \neq 1$ , 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	$x$	$x + 1$	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  $\text{GF}(28)$  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. (a)  $R = [8\ 1\ 4\ 5\ 7\ 6\ 3\ 2]$

(b)  $r_i = j$  if and only if  $p_j = i$ , for  $1 \leq i \leq n$ .