Suggested Solutions to Homework Assignment #1A

(prepared by Willy Chang)

1. Exercise problems from [Stallings 6E Intl.]:

1.1 The system must keep personal identification credentials confidential, both in the host system and during any transcations (like query, update, etc.). It must protect the integrity of account records and of individual transactions per student ID, or anything unique to a student. Availability of the host system is important to the instructors, and maybe departments of student affairs. The availability of an individual student is of less concern.

2.1 **a**. $C_1 = E([4,6],0) = (4 \times 0 + 6) \bmod 26 = 6$
$C_2 = E([4,6],13) = (4 \times 13 + 6) \bmod 26 = 6$

b. It is not an one-to-one algorithm. According to the definition, decryption is impossible.

c. The Caesar cipher is not one-to-one for all values for **a**. 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 $q = p + m/k \neq p$.

2.18 **a**. The cipher result is as following:

plaintext	c	r	y	p	t	o	g	r	a	p	h	y
+key	10	22	5	4	1	0	2	9	18	16	16	0
ciphertext	M	N	D	T	U	O	I	A	S	F	X	Y

So the ciphertext will be ”MNDTUOIASFXY”.

b. Reverse the work as following:

ciphertext	M	N	D	T	U	O	I	A	S	F	X	Y
-plaintext	a	p	p	l	i	c	a	t	i	o	n	s
key	12	24	14	8	12	12	8	7	10	17	10	6

So the specified key will be ”12 24 14 8 12 12 8 7 10 17 10 6”.

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.

3.4 **a**. We need only to determine the probability that not all the remaining plaintexts exactly agree between $E(K, \cdot)$ and $E(K', \cdot)$. That is, $\neg(\forall P_i.\ t+1 \leq i \leq N \rightarrow E[K, P_i] = E[K', P_i])$. So the probability that $E(K, \cdot)$ and $E(K', \cdot)$ are in fact distinct mappings is $1 - 1/(N-t)!$.

b. We say that a permutation π has a fixed point at m if $\pi(m) = m$. To simplify the question, we may assume that $E[K, P_i] = P_i$ without loss of generality. It then follows that we seek the probability for having a permutation on $N - t$ objects that has exactly t' fixed points, while none of the remaining $N - t - t'$ ones are fixed. Then according to the calculations we've learned at secondary school, let $N - t - t'$ be r,

$$\Pr(t' \text{ additional fixed points in } N - t)$$

$$= \text{ways } t' \text{ out of } N - t \times \Pr(\text{given certain } t' \text{ objects, no fixed points in } N - t - t')$$

$$= C_{t'}^{N-t} \times \frac{r! - C_1^r(r-1)! + C_2^r(r-2)! - C_3^r(r-3)! + \ldots C_r^r 0!}{(N-t)!}$$

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

3.8 **a**. Let's work this from the inside out.

$T_{16}(L_{15}||R_{15}) = L_{16}||R_{16}$
$T_{17}(L_{16}||R_{16}) = R_{16}||L_{16}$
$IP[IP^{-1}(R_{16}||L_{16})] = R_{16}||L_{16}$
$\rightarrow TD_1(R_{16}||L_{16}) = R_{15}||L_{15}$

b. Similar with above.

$T_{16}(L_{15}||R_{15}) = L_{16}||R_{16}$
$IP[IP^{-1}(L_{16}||R_{16})] = L_{16}||R_{16}$
$TD_1(R_{16}||L_{16}) = R_{16}||L_{16} \oplus f(R_{16}, K_{16})$
$\neq L_{15}||R_{15}$

4.14 We have
$1 \equiv 1 \pmod 9$; $10 \equiv 1 \pmod 9$;
$10^2 \equiv 10(10) \equiv 1(1) \equiv 1 \pmod 9$; $10^{n-1} \equiv 1 \pmod 9$.
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 1279 mod 9721, gcd(1279, 9721) is calculated using the Extended Euclidean algorithm. The following table lists the stages of the algorithm:

i	r	q	x	y
−1	1279		1	0
0	9721		0	1
1	1279	0	1	0
2	768	7	−7	1
3	511	1	8	−1
4	257	1	−15	2
5	254	1	23	−3
6	3	1	−38	5
7	2	84	3215	−423
8	1	1	−3253	428
9	0	2		

Thus, the multiplicative inverse of 1279 mod 9721 is 6468.

b. In order to find the multiplicative inverse of 729 mod 311, gcd(729, 311) is calculated using the Extended Euclidean algorithm. The following table lists the stages of the algorithm:

i	r	q	x	y
−1	729		1	0
0	311		0	1
1	107	2	1	−2
2	97	2	−2	5
3	10	1	3	−7
4	7	9	−29	68
5	3	1	32	−75
6	1	2	−93	218
7	0	3		

Thus, the multiplicative inverse of 729 mod 311 is 218.

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

		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^3+x in GF(2^4) with $m(x) = x^4+x+1$, gcd(x^4+x+1, x^3+x) 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^4+x+1		1	0
0	x^3+x		0	1
1	x^2+x+1	x	1	x
2	$x+1$	$x+1$	$x+1$	x^2+x+1
3	1	x	x^2+x+1	x^3+x^2
4	0	$x+1$		

$(x^2+x+1)\dot{(}x^4+x+1)+(x^3+x^2)\dot{(}x^3+x) = 1$
Thus, the multiplicative inverse of x^3+x under the conditions of the question is x^3+x^2.

2. (a) R = [7 2 4 1 8 6 3 5]

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