CSCI 556: Introduction to Cryptography
Homework – 2

1.
$$c1 = m1 \oplus k$$
$$c2 = m2 \oplus k$$
$$c3 = m3 \oplus k$$

If c1, c2 and c3 is known then we can get little info about m1, m2 and m3

$$c1 \oplus c2 = m1 \oplus k \oplus m2 \oplus k$$

- ⇨ $c1 \oplus c2 = m1 \oplus m2$ (because $k \oplus k = 1$)
- ⇨ $c2 \oplus c3 = m2 \oplus m3$ (because $k \oplus k = 1$)
- ⇨ $c1 \oplus c3 = m1 \oplus m3$ (because $k \oplus k = 1$)

But if Alice gets to know m1 then all the information is compromised now. She can easily decode everything with the use of c1, c2, c3 and m1. With c1 and m1, she can get to know about key k and once she knows k, she can easily get to know m2 and m3 as well.

$c1 \oplus m1 = m1 \oplus k \oplus m1$ (Using c1 and m1)
$\Rightarrow c1 \oplus m1 = k$
$c2 \oplus k = m2 \oplus k \oplus k$ (Using c2 and k calculated above)
$\Rightarrow c2 \oplus k = m2$
$c3 \oplus k = m3 \oplus k \oplus k$ (Using c3 and k calculated above)
$\Rightarrow c3 \oplus k = m3$

2. Last two digits of:
   i. 76^ (any natural number) is always 76
   ii. 24^odd is always 24
   iii. 24^even is always 76

$4^{100} = (2^2)^{100} = 2^{200}$
$= (2^{10})^{20}$
$= (24)^{20}$ (because last two digits of $2^{10} = 24$)
$= 76.$ (according to above facts)

Last two digits of $4^{100} = 76$

3

1. f: $\{0, 1\}^{n} \rightarrow \{0, 1\}^{2n}$

ii. $f(\langle a \rangle) = \langle a^2 \bmod N \rangle \,||\, \langle a^3 \bmod N \rangle$

I. Let's consider term1 = $\langle a^2 \bmod N \rangle$ and term2 = $\langle a^3 \bmod N \rangle$.
II. $f(\langle a \rangle)$ = term1 || term2.
III. As we can see $f(\langle a \rangle)$ is not random.
IV. That is, if we computer term1 then we can easily compute term2 by just raising it to 3/2 or by multiplying it with $\langle a \rangle$ again. This is clearly not random since term2 depends on term1
V. Because of the above reasons, I don't think $f(\langle a \rangle)$ is a pseudo-random generator.

4. $G(x, y) = (x^2 \bmod N, y, b)$

b = $\oplus$ of last bit of x and last bit of y

I. We know x^2 mod N => we know last bit of x
II. We know last bit of x and we already y => we know b value
III. So, b is indeed a hard code bit and it's not random
IV. Because of above reasons G(x, y) is not a pseudo-random generator

5.

Yes, matrix cipher is vulnerable to plain text attack. Let's say we have a plain-message vector [x, y] and a 2*2 matrix cipher of unknowns along with a encrypted message vector [p, q]. The attacker already knows the plain-message vector [x, y] and encrypted message vector [p, q]. He only has to decrypt the 2*2 matrix cipher.

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} p \\ q \end{bmatrix}$$

If we solve now, we get 2 equations:

$$ax + by = p$$
$$cx + dy = q$$

Attacker already knows x, y, p, q. Only a, b, c, d has to be deduced. Since now the equation has been reduced to linear time or specifically polynomial time, it can be solved by machines. Hence Matrix Cipher is vulnerable to plain-text attack.