James Thurlow/Matt Bell

CSCI 345 Homework 1

5 February 2018

Dr. Mountrouidou

(For part 3 below)

James Blog Link: https://jamesthurlowblog.blogspot.com/

Matt Blog Link: https://20f1ware3ngin33ring.wordpress.com/

Part 2: Cryptography

1. DES

(weak DES keys) There are four so called weak DES keys. One of those keys is K = 00011111 00011111 00011111 00011111 00001110 00001110 00001110 00001110.
a) What happens if you use this key?

```
1F1F 1F1F 0E0E 0E0E
```

If you use this type of key, it causes the encryption mode of DES to act like the decryption mode thus revealing the plain text you were trying to hide in the first place.

b) Can you find the other three weak keys?

```
0101 0101 0101 0101
```

```
E0E0 E0E0 F1F1 F1F1
```

```
FEFE FEFE FEFE FEFE
```

2. RSA

In this exercise we consider an RSA modulus n = p x q where p and q are large prime numbers (here, by large we mean at least equal to 5). We consider a valid RSA exponent e for RSA.

a. ***Show that neither (p mod 3) nor (q mod 3) can be equal to 0***

We assume p and q to be prime and large. Since 3 is prime itself, and p and q are much much larger than 3 then for x mod 3 to be equal to zero x must either be three, zero, or a multiple of three. A multiple of three by definition cannot be prime.
ex:
7 mod 3 = 1
5 mod 3 =2

b. ***Under which condition e is a valid exponent for a modulus n?***

$d \cdot e \equiv 1 \pmod{\lambda(n)}$.

c. ***From now on, we will assume that e=3 . Show that neither p-1 nor q-1 can be multiples of 3***

$a^{(p-1)(q-1)} \equiv 1 \bmod pq$
P = 11
Q=2
11 mod 3 = 2 , 2 mod 3 = 2
Fermat's theorem

d. ***Deduce that p mod 3 = q mod 3 = 2.***

e. ***What is the value of n mod 3?***

P=11
Q= 2
P*Q= 22 which is N
22 mod 3 = 1

3. Elliptic Curve

List the points on the elliptic curve E: $y^2 = x^3 - 2 \pmod 7$

The points are (3,2), (3,5), (5,2), (5,5), (6,2), (6,5)