MATH 178 Homework #10

Tamir Enkhjargal

May 2019

My color: Red, My partner's color: Blue

RSA

1.

$p = 7,\ q = 97,\ e = 257,\ n = pq = 679,\ \varphi(679) = \varphi(7)\varphi(97) = 96 * 6 = 576.$

$$d = e^{-1}(\text{mod} 576) \equiv 1 \tag{1}$$

$$576 = 2 * 257 + 62 \tag{2}$$
$$257 = 4 * 62 + 9 \tag{3}$$
$$62 = 6 * 9 + 8 \tag{4}$$
$$9 = 1 * 8 + 1 \tag{5}$$

$$1 = 9 - 1 * 8 \tag{6}$$
$$1 = 9 - 1(62 - 6 * 9) \tag{7}$$
$$1 = 7 * 9 - 62 \tag{8}$$
$$1 = 7(257 - 4 * 62) - 62 \tag{9}$$
$$1 = 7 * 257 - 29 * 62 \tag{10}$$
$$1 = 7 * 257 - 29 * (576 - 2 * 257) \tag{11}$$
$$1 = 65 * 257 - 29 * 576 \tag{12}$$
$$1 = 65 * 257 \tag{13}$$
$$d = 65 \tag{14}$$

To decrypt 146, use 146^{65} mod (679)

Reduce $146^{65}(\text{mod } 679)$

$b = 65,\ n = 146,\ m = 679,\ S[\ ] = \{1, 0, 0, 0, 0, 0, 1\},\ k = 6$

$n(\text{mod} 679)$	s	a
		1
146	s[0]=1	146
146^2=267	s[1]=0	146
267^2=673	s[2]=0	146
673^2=36	s[3]=0	146
36^2=617	s[4]=0	146
617^2=449	s[5]=0	146
449^2=617	s[6]=1	454

To decode 454 to a key pair a, b, use $146/26 = 17 = a$, 146 mod $26 = 12 = b$.

Now we have the encrypting pair a, b we need to find the decrpyting pair a', b'

$$26 = 1 * 17 + 9 \tag{1}$$

$$
\begin{aligned}
17 &= 1 * 9 + 8 \qquad \tag{2}\\
9 &= 1 * 8 + 1 \qquad \tag{3}
\end{aligned}
$$

$$
\begin{aligned}
1 &= 9 - 1 * 8 \tag{4}\\
1 &= 9 - (17 - 1 * 9) \tag{5}\\
1 &= 2 * 9 - 17 \tag{6}\\
1 &= 2(26 - 1 * 17) - 17 \tag{7}\\
1 &= 2 * 26 - 3 * 17 \tag{8}\\
1 &= -3 * 17 \tag{9}\\
1 &= 23 * 17 \tag{10}
\end{aligned}
$$

We can now decrypt the message. Using the encoding $a = 0, b = 1...$

$$
\begin{aligned}
P &\equiv a'(C - b)(\text{mod} 26) && \tag{1}\\
&\equiv 23(C - 12)(\text{mod} 26) && \tag{2}\\
P &\rightarrow 23(15 - 12)(\text{mod} 26) && = 17 = R \tag{3}\\
B &\rightarrow 23(1 - 12)(\text{mod} 26) && = 7 = H \tag{4}\\
E &\rightarrow 23(4 - 12)(\text{mod} 26) && = 24 = Y \tag{5}\\
X &\rightarrow 23(23 - 12)(\text{mod} 26) && = 19 = T \tag{6}\\
B &\rightarrow 23(1 - 12)(\text{mod} 26) && = 7 = H \tag{7}\\
I &\rightarrow 23(8 - 12)(\text{mod} 26) && = 12 = M \tag{8}
\end{aligned}
$$

The original plaintext was `RHYTHM`.

Using a new encrypting pair $a, b = \{11, 21\}$. $11 * 26 + 21 = 307$. To encrypt this, reduce 307^{19} mod 681.

Reduce $307^{19}(\text{mod } 681)$

$b = 19,\ n = 307,\ m = 681,\ S[\ ] = \{1, 0, 0, 1, 1\},\ k = 4$

$n(\text{mod} 681)$	s	a
		1
307	s[0]=1	307
307^2=271	s[1]=1	307
271^2=574	s[2]=0	115
574^2=553	s[3]=0	115
553^2=40	s[4]=1	514

The reduced number that I would send to (you) is 514.

2.

p =`50453156304734882643265661554998829784271380864981`
n =`1859486070465862481250084737025244499643330...2729`
q =`36855693610814891619906843543364439878667990665909`
e =`5746381426879165805597951012558256671104182...7277`
$\varphi(n)$ =`1859486070465862481250084737025244499643...1840`
d =`1781807991792385566284160318478558467393146...9173`

3.

The message is:
53285491632384029814060608150978435305953163003130
0070853873325328959028610977865082224016588557854.

This was the encryption $m^e \pmod n$. Therefore to decrypt we need $m^d \pmod n$. `Mod(c,n)^d=9260`. This is our key.

The ciphertext was 7FCF82CF65F8F607EB4B9D7CFA....

Therefore, our plaintext was:

```
fresh freaken crawdad.  whats my middle name.
```

4.

Since my partner's color is ***blue***, he also has a different n and e.

The key is 51913.

`Mod(m,n)^e`=1663...7914

The key is 51914.

`Mod(m,n)^e`=9656...1560

4.5.

Person 1 → $n_1 = r_1 r_2$
Person 2 → $n_2 = r_1 r_2$
Person 3 → $n_3 = r_3 r_4$
Person 4 → $n_4 = r_3 r_5$

i) Person 2 is a danger to Person 1, because they share the same n, p, q. This means that Person 2 can decode any of Person 1's private messages.

ii) If all of the n_i are the same, and one prime was being shared, r_3, r_4, r_5 specifically, then $r_5 = r_4$ if they are sharing the same n and r_3. This means that Person 4 is a danger to Person 3.