M 375 – Homework 4

11.2.1

Intercepted cryptogram: $c = 10$. Public key $e = 5$ and $n = 35$

- Factorize $n = 35 = 5 \cdot 7$.
- Compute $(p-1)\cdot(q-1) = 4 \cdot 6 = 24$.
- Solve $5d \equiv 1 \bmod 24 \Rightarrow d = 5$.
- Decrypt $m \equiv c^d \bmod n \Rightarrow m \equiv 10^5 \bmod 35 \Rightarrow m = 5$.

The secret message is $m = 5$.

11.2.2

Public key $e = 31$ and $n = 3599$.

- Factorize $n = 3599 = 59 \cdot 61$.
- Compute $(p-1)\cdot(q-1) = 58 \cdot 60 = 3480$.
- Solve $31d \equiv 1 \bmod 3480 \Rightarrow$ $31x - 3480y = 1$

$$
\begin{aligned}
3480 &= 112 \cdot 31 + 8 \\
31 &= 3 \cdot 8 + 7 \\
8 &= 1 \cdot 7 + 1
\end{aligned}
$$

$$
\begin{aligned}
1 &= 8 - 1 \cdot 7 \\
&= 8 - 1 \cdot (31 - 3 \cdot 8) \\
&= (3480 - 112 \cdot 31) - 1 \cdot (31 - 3 \cdot (3480 - 112 \cdot 31)) \\
&= 3480 - 112 \cdot 31 - 31 + 3 \cdot 3480 - 336 \cdot 31 \\
&= 4 \cdot 3480 - 449 \cdot 31 \\
\Rightarrow\ & d = 3480 - 449 = 3031.
\end{aligned}
$$

p. 196, problem 1

Bob's public key $e_B = 43$ and $n = 77$. The intercepted cryptogram is $c = 5$.

- Factorize $n = 77 = 7 \cdot 11$.
- Compute $(p-1)\cdot(q-1) = 6 \cdot 10 = 60$.
- Solve $43d \equiv 1 \bmod 60 \Rightarrow d = 7$ (see 11.2.2 for method of solving this equation).
- Decrypt $m \equiv c^d \bmod n \Rightarrow m \equiv 5^7 \bmod 77 \Rightarrow m = 47$.

p. 197, problem 9

(i) Solving $x^2 \equiv d \bmod pq$ is the same as solving $dy^2 \equiv d \bmod pq$ (substitute $y^2 = d^{-1}x^2$).

$$\Rightarrow \begin{cases} y^2 \equiv 1 \bmod p \\ y^2 \equiv 1 \bmod q \end{cases}$$

$$\Rightarrow \begin{cases} y \equiv \pm 1 \bmod p \\ y \equiv \pm 1 \bmod q \end{cases}$$

This leads to 4 equations; each equation yields one solution:

$y \equiv +1 \bmod p \equiv +1 \bmod q \equiv +1 \bmod pq$

$y \equiv -1 \bmod p \equiv -1 \bmod q \equiv -1 \bmod pq$

$y \equiv +1 \bmod p \equiv -1 \bmod q \equiv w \bmod pq$

$y \equiv -1 \bmod p \equiv +1 \bmod q \equiv z \bmod pq.$

(ii) Choose $p = 3$, $q = 5$, and $d = 6$, then $x^2 \equiv 6 \bmod 15$ has only two solutions ($x_1 = 6, x_2 = 9$).

p. 198, problem 12

Message *m*, $1 \le m \le n-1$, and $m^e \equiv m \bmod n$ (*m* is a fixed point; it is encrypted to itself). Show that $(n-m)^e = (n-m) \bmod n \equiv -m \bmod n$ ($n-m$ is also a fixed point).

$$(n-m)^e = \left(a_0 n^e + a_1 n^{e-1} m + \ldots + a_{e-1} n m^{e-1} + a_e m^e\right) \bmod n$$

Since every term of this (polynomial) sum with some power of *n* is 0 ($\bmod n$)

$$(n-m)^e \bmod n = a_e m^e$$

and since *e* is an odd power (only odd powers are used to encrypt)

$$a_e = -1 \text{ and } (n-m)^e \bmod n \equiv -m^e \bmod n \Rightarrow$$

$$-m^e \equiv -m \bmod n.$$

p. 198, problem 13

The equation $m^e \equiv m \bmod pq$ splits up into a system of two equations:

$$\begin{cases} m^e \equiv m \bmod p \\ m^e \equiv m \bmod q \end{cases} \qquad (1)$$

$$\Rightarrow \qquad \begin{cases} m^{e-1} \equiv 1 \bmod p \\ m^{e-1} \equiv 1 \bmod q \end{cases} \qquad (2)$$

$$\Rightarrow \qquad \begin{cases} e-1 \equiv 0 \bmod (p-1) \\ e-1 \equiv 0 \bmod (q-1) \end{cases} \qquad (3)$$

The number of events (i.e. how often $e-1 \equiv 0 \bmod x$) in (3) is

$\gcd(e-1, p-1) = r$ for the first equation and

$\gcd(e-1, q-1) = s$ for the second equation.

So for $p \cdot q$ it happens $r \cdot s$ times.

Dividing (or multiplying by the inverse) by *m* in (1) is not always possible. There are *m*'s that don't have an inverse. We have to look separately at these *m*'s. There are *r* such *m*'s for the first equation and *s* such *m*'s for the second equation. So the total number of *m*'s (*m* is a fixed point, see problem 12) is

$r + s + rs$.