Public Key Encryption

1 The Algorithm

Here are the steps to encode/decode using Public Key Encryption.

1. Spy Boss picks some coding constants:
   (a) p, q large primes.
   (b) Let $N = pq$
   (c) Find $e \in \mathbb{N}$ with $\gcd(e, p-1) = \gcd(e, q-1) = 1$.
   (d) Find $d \in \mathbb{N}$ with $ed \equiv 1 \mod (p-1)(q-1)$
   (e) (N, e) is the public key and is shared with all.

2. Spy and Boss agree upon a code of converting letter to numbers and back. Here's my encoding:

```
abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789 .,;:?-'"()!@#$%^&*‘=+
12345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234
        10        20        30        40        50        60        70        80
```

   The way to read this is the top line is the letter/symbol to encode, the next two lines tell you the number. So, for example we have a=1, b=2, ..., A=27, ..., [space]=23, '.'=24, etc.

3. Spy converts his message into numbers, padding each number (if necessary) so that each letter takes 2 digits of the big number. The spy then concatenates these numbers together to make blocks of numbers (the size of these blocks depends on N). If N is big enough or the message is short enough, the spy might just have one large number to encode.

4. For a given block of numbers, X, the spy can encode these as:

$$y = x^e \mod N$$

   The y, is the coded message.

5. The Boss received the message and decodes the message:

$$x = y^d \mod N$$

   The mathematics ensures that $(x^e)^d = x^{ed} \equiv x \mod N$.

2 An Example

1. Boss picks:
   (a) $p = 11$, $q = 13$
   (b) $N = 143$
   (c) $e = 7$
   (d) $d = 103$
   (e) $(N, e) = (143, 7)$ is shared with everyone.
2. The coding of {Letters} $\leftrightarrow$ {Numbers} is described above.
3. The Spy's message is: "Beware of Sarumon"

B	e	w	a	r	e		o	f		S	a	r	u	m	o	n
28	5	23	1	18	5	63	15	6	63	45	1	18	21	13	15	14

   This could be encoded into a single number:

   $$28052301180563150663450118211315 14$$

   But, reducing mod N would lose all the information. Because N is so small we can really only encode one number at a time. Thus, each block of numbers to encode is really only one letter of the message (two digits at most). (Obviously, this makes the message less secure.)
4. Each number is raised to the power of $e = 7$ and reduced mod $N =$ mod 143:

Letter	B	e	w	a	r	e		o	f		S	a	r	u	m	o	n
x	28	5	23	1	18	5	63	15	6	63	45	1	18	21	13	15	14
x^e	63	47	23	1	138	47	2	115	85	2	111	1	138	109	117	115	53

5. The Boss receives the message:

   $$\text{Code:} \quad 63, 47, 23, 1, 138, 47, 2, 115, 85, 2, 111, 1, 138, 109, 117, 115, 53$$

   The Boss uncodes each number, y by y^d, and then converts the number to a letter:

y	63	47	23	1	138	47	2	115	85	2	111	1	138	109	117	115	53
y^d	28	5	23	1	18	5	63	15	6	63	45	1	18	21	13	15	14
Letter	B	e	w	a	r	e		o	f		S	a	r	u	m	o	n

   The Boss receives the message "Beware of Sarumon" and, accordingly, is wary of his dealings with the White Wizard.

3 Exercises

1. You're the Boss. Your public key is $(N, e) = (119, 77)$. Your private key is $d = 5$. Decode the following messages:

   (a) 11,25,56,91

   (b) 2,86,36,72,36

   (c) 101,1,56,72,1,31,27

2. You're the Spy with public key $(119, 77)$. Encode the following messages:

   (a) Smaug

   (b) Mordor

3. Let $p = 5$ and $q = 7$ (These are too small for any actual encoding example)

   (a) Find all possible values for e that will work to encode.

   (b) For each of your e, find the corresponding d to decode.

4. You just intercepted a message from the enemy! You have to decode it. You know the public key is $(10057, 4549)$.
   The message you intersepted is

   $$3849, 1634, 5273, 6073, 6417, 5284, 3907$$

   Decode it!