Math135 - November 11'th, 2015
RSA - Example And Proof

Example:

Suppose Alice chooses $p = 11$, $q = 13$, $e = 23$.

1) What is Alice's public key?
2) What is Alice's private key?
3) If Bob wants to send message $M = 25$ to Alice, what is ciphertext C?

1) Alice's public key is (e, n)
   $n = pq$
   $n = (11)(13)$
   $n = 143$
   Alice has already chosen e such that $1 < e < (p-1)(q-1)$ and $\gcd(e, (p-1)(q-1)) = 1$.
   So, public key is $(23, 143)$
2) To get private key d, we must solve
   $ed \equiv 1 \pmod{120}$
   $23d \equiv 1 \pmod{120}$

   We'll use EEA to solve this.

$$23d \equiv 1 \pmod{120}$$
$$23d - 1 = 120k, k \in \mathbb{Z}$$
$$120k + 23d = 1$$

k	d	r	q
1	0	120	0
0	1	23	0
1	-5	5	5
-4	21	3	4
5	-26	2	1
9	47	1	1
23	-120	0	2

So, $d = 47$.

3) To encode the message, we need to solve the following congruence:

$$25^{23} \equiv C \pmod{143}$$
$$25^{16}25^{4}25^{2}25 \equiv C \pmod{143} \text{ (Calculate these off to the side)}$$
$$(14)(92)(53)(25) \equiv C \pmod{143}$$
$$(1288)(1325) \equiv C \pmod{143}$$
$$(1)(38) \equiv C \pmod{143}$$
$$38 \equiv C \pmod{143}$$

   Because $C < 143$, $C = 38$.

   Note: If Alice wanted to decrypt message C, she must solve:
   $38^{47} \equiv 25 \pmod{143}$

RSA Theorem

If:

1) p and q are prime numbers.
2) $n = pq$
3) e and d are positive integers such that $ed \equiv 1 \pmod{(p-1)(q-1)}$
4) $0 \leq M \leq n$
5) $M^e \equiv C \pmod{n}$
6) $C^d \equiv R \pmod{n}$ Where $0 \leq R \leq n$

Then, $R = M$.

RSA Theorem - Proof

Assume all hypothesis of the RSA Theorem (1-6).

$$\begin{aligned} R &\equiv C^d \pmod{n} \text{ (By hypothesis)} \\ &\equiv M^{e^d} \pmod{n} \text{ (By hypothesis)} \\ &\equiv M^{ed} \pmod{n} \end{aligned}$$

We know:

$$\begin{aligned} ed &\equiv 1 \pmod{(p-1)(q-1)} \\ &= 1 + k(p-1)(q-1), k \in \mathbb{Z} \end{aligned}$$

$$\begin{aligned} \text{So, } R &\equiv M^{1+k(p-1)(q-1)} \pmod{n} \\ &\equiv M \cdot M^{k(p-1)q-1)} \pmod{n} \end{aligned}$$

Since $p \mid n$ and $q \mid n$, we know:

$\equiv M \cdot M^{k(p-1)(q-1)} \pmod{p}$ and $R \equiv M \cdot M^{k(p-1)(q-1)} \pmod{q}$

We will show $\equiv M \pmod{p}$ and $R \equiv M \pmod{q}$

Case 1: $p \mid m$
$M \equiv 0 \pmod{p}$
and $m \cdot M^{k(p-1)(p=1)} \equiv 0 \pmod{p}$
So, $R \equiv M \pmod{p}$

Case 2: $p \nmid m$

$$\begin{aligned} M^{p-1} &\equiv 1 \pmod{p} \text{ (By F}\ell\text{T)} \\ (M^{(p-1)})^{k(q-1)} &\equiv 1^{l(q-1)} \equiv 1 \pmod{p} \\ M \cdot M^{k(p-1)(q-1)} &\equiv M \pmod{p} \end{aligned}$$

$R \equiv M \pmod{p}$ (By Transitivity of Congruences)

In a similar manner, we show $R \equiv M \pmod{q}$.

Since $\gcd(p, q) = 1$, then $R \equiv M \pmod{pq}$ (CRT)

And, since $n = pq$, $R \equiv M \pmod{n}$

As $0 \leq R, M \leq n$, $R = M$

Why is RSA Secure?

Given (e, n) (The public key) and C, the ciphertext (or encrypted message), we need to find d to decrypt.
To find d, you need $(p-1)(q-1)$, which means factoring n. This is a very difficult task for computers, especially with large n. This means an eavesdropper has no efficient method of computing d and decoding the message.