An Introduction to RSA

David Boyhan

August 5, 2008
For 2000 Years ...

- Encryption was symmetric:
  - \( E(M, k) \rightarrow C \)
  - \( D(C, k) \rightarrow M \)

- The same key \( k \) is used for both steps

- Example: Caesar’s Shift Cipher, with \( k = 3 \)
  - \( \text{DM HURTS MY BRAIN} \Rightarrow \text{GP KXUWV OB EUDLQ} \)

- Symmetric Ciphers:
  - Are subject to interception
  - Require expensive key distribution

- The same issue exists for steganography and one-time pads.
Diffie & Hellman Invent PKC

- In 1977, Whitfield Diffie and Martin Hellman published *New Directions in Cryptography* proposing a public-key cryptography scheme.

- They propose:
  - $E(M, e) \rightarrow C$
  - $D(C, d) \rightarrow M$
  - $D(C, e) \not\rightarrow M$

- One key $e$ locks

- One key $d$ unlocks

- $e$ is the public key. $d$ is the private key

- They keys are linked, but $d$ cannot be derived from $e$. 
**Trap Door Problems**

Diffie & Hellman suggest use of **trap door** or **one-way** problems.

Example:

1. Multiply 13,719 by 23,546 to get 323,041,293

2. Now, factor 323,041,292 into its prime factors of \(3^2 \times 17 \times 47 \times 167 \times 269\)

Diffie & Merkle attempt use of knapsack problems for the trap door. This is proven to be cryptographically insecure.
Enter RSA

- In 1978, Ronald Rivest, Adi Shamir and Leonard Adelman (RSA) publish *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*. This becomes the de facto standard for public-key cryptography for 30 years.

- The trap-door is based on factoring of large numbers and modular mathematical inverse.

- The basic algorithm requires creation/selection of 5 integers:
  - $p$ and $q$ are large prime numbers
  - $n$ which is generated by $p \cdot q$
  - $d$ which is relatively prime to $(p - 1) \cdot (q - 1)$
  - $e$ which is generated by $d$ and $n$

- $M$ is the original message. $C$ is the cipher-text
The RSA Algorithm

The algorithm is **amazingly** simple:

“. . ., the result (the ciphertext $C$) is the remainder when $M^e$ is divided by $n$. To decrypt the ciphertext, raise it to another power $d$ again modulo $n$.”

$$E(M) = M^e \pmod{n} = C$$

$$D(C) = C^d \pmod{n} = M$$
The Hard Parts ...

- Selecting \( p \) and \( q \) requires rapid testing for primality. This is not too hard.
- Selecting \( d \) as \( \gcd(d, ((p - 1) \cdot (q - 1))) = 1 \) requires basic algorithm (min is fine, Euclid’s Algorithm is also used)
- Creating \( e \) is the complex part (at least for me), because:

\[ e \text{ is the multiplicative inverse of } d \mod ((p - 1) \cdot (q - 1)) \]

- To find modular multiplicative inverse, we need to find \( e \) such that \( d \cdot e = 1 \mod ((p - 1) \cdot (q - 1)) \)
- To do that, we need Euler’s Totient and Euler’s Generalization of Fermat’s Little Theorem
Euler’s Totient

- Euler’s Totient of \( n, \phi(n) \), is defined as the number of positive integers less than \( n \) that are relatively prime to \( n \).

- If \( n \) is prime then \( \phi(n) \) is simply \( (n - 1) \). If both \( p \) and \( q \) and prime, then it’s easy to see that \( \phi(p \cdot q) \) will be \( ((p - 1) \cdot (q - 1)) \).

- Example if \( n \) is not prime - there are 4 numbers that are relatively prime to 12, being \((1, 5, 7, 11)\). Therefore \( \phi(12) \) is 4.

- Calculating Euler’s Totient \( \phi(n) \) can be done through the prime factorization of \( n \) such that \( n = p_1^{k_1} \cdots p_r^{k_r} \).
Euler’s Totient (continued)

- We then identify the distinct primes and compute $\phi(n)$ using the following formula:

$$n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

- Therefore, for example, $12 = 2^2 \cdot 3^1$ so the Totient would be

$$12 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{3}\right) = 12 \cdot \frac{1}{2} \cdot \frac{2}{3} = 4.$$  

- Similarly, because the prime factorization of $54 = 2^1 \cdot 3^3$ then $\phi(54)$ would also be

$$54 \cdot \frac{1}{2} \cdot \frac{2}{3} = 18.$$
Euler’s Generalization of Fermat’s Little Theorem

- Euler’s Generalization of Fermat’s Little Theorem states that: if $gcd(d, z) = 1$ then $d^{\phi(z)} \mod z = 1$. This is a condition we have already satisfied with $d$ and $((p - 1) \cdot (q - 1))$.

- Substituting $((p - 1) \cdot (q - 1))$ for $z$ we can see, using Fermat’s Little Theorem that:

  \[ 1 = d^{\phi((p-1)\cdot(q-1))} \mod ((q - 1) \cdot (p - 1)) \]
Euler’s Generalization (continued)

- We also know that based on the definition of multiplicative modular inverse that:

$$e \cdot d = 1 \pmod{(p - 1) \cdot (q - 1)}$$

$$e \cdot d \cdot d^{-1} = d^{-1} \cdot 1 \pmod{(p - 1) \cdot (q - 1)}$$

Substituting in $$d^{\phi((p-1)\cdot(q-1))} \pmod{((q - 1) \cdot (p - 1))}$$ for $$1 \pmod{(p - 1) \cdot (q - 1)}$$, we get:

$$e \cdot 1 = d^{\phi((p-1)\cdot(q-1))^{-1}} \pmod{(p - 1) \cdot (q - 1)}$$
Example

- To create \( n \) we’ll use: \( p = 5, q = 11 \). \( n = p \cdot q = 5 \cdot 11 = 55 \).

- Pick random number that is relatively prime to \( ((p - 1) \cdot (q - 1)) = d = 7 \).

- We calculate \( e \) using \( d \) and Euler’s Generalization of Fermat’s Little Theorem. Accordingly:

\[
e = d^{\phi((p-1)\cdot(q-1))^{-1}} \mod ((p - 1) \cdot (q - 1)) = 7^{\phi(4 \cdot 10)^{-1}} \mod 4 \cdot 10
\]

- \( 40 = 2^3 \cdot 5^1 \), therefore, \( \phi(40) = 40 \cdot (1 - \frac{1}{2}) \cdot (1 - \frac{1}{5}) = 40 \cdot \frac{1}{2} \cdot \frac{4}{5} = 16 \)

- Therefore, \( e = 7^{15} \mod 40 \) and \( e = 23 \). 

Finally we’ll start with plain-text message $M$:DM HURTS MY BRAIN

For the purposes of this example, we’ll use the integers 1-26 to represent the alphabet and remove all spaces. However, under normal circumstances, ASCII would be used instead. Therefore, $M$ becomes: D M H U R T S M Y B R A I N

$\Rightarrow 04\ 13\ 08\ 21\ 18\ 20\ 19\ 13\ 25\ 02\ 18\ 01\ 09\ 14$

First encrypted block $C_1 = 04^{23} \pmod{5}5 = 09$

The entire message is encrypted as: $09\ 52\ 17\ 21\ 02\ 25\ 39\ 52\ 05\ 08\ 02\ 01\ 14\ 49$

To decrypt, reverse the process with $D(C) = C^d \pmod{n} = M$
The Consequences of RSA

• $33 billion in e-commerce transactions for 1st quarter 2008
• In 1991 PGP makes strong cryptography available to everyone
• Philip Zimmermann gets sued and investigated by the FBI
• The US Government proposes the Clipper Chip
• Philip Zimmermann gets an RSA license and the FBI drops the case
• The US Government drops Clipper Chip
• PGP and GNU Privacy Guard are world-wide
• The 2008 Summer Olympics remain ...