RSA Cryptography: Our World's Security

Seth Hamilton

Valparaiso University

July 25, 2017

Motivation

- During my freshman year, I heard a talk on Cryptography.
- The presentation was very interesting and blended the ideas of computer science with mathematics.
- The Imitation Game was also a part in my interest in encryption and decryption of codes.

History

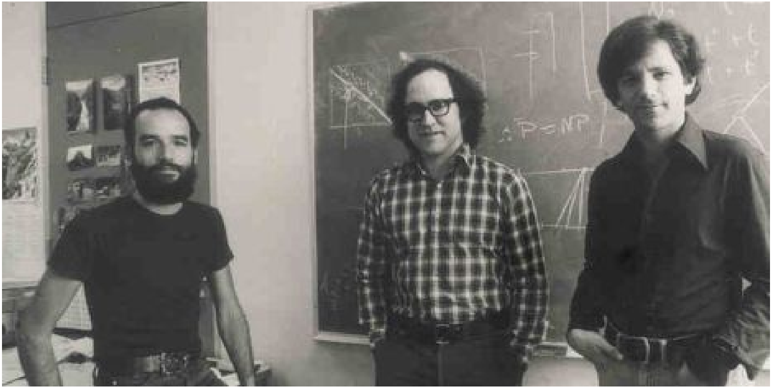
- Cryptography is the subject of transforming information, so it cannot be easily recovered without special knowledge.
- Julius Caesar is one of the first known people to use cryptography.
- He shifted the letters of the alphabet in order to encrypt messages he was sending.
- Originally, cryptography would be a system that could be represented as a receiver receiving many messages (locks) and having to keep track of many different keys that go to these locks in order to break them.

History

- James Ellis came up with an idea that would allow a public distribution of open locks all with the same key, but the locks could have a message kept inside then sent back to the person with the key so only he/she can open the lock and read the message.
- Sadly, Ellis was unable to come up with a mathematical solution to his idea.

History

- Ronald Rivest, Adi Shamir, and Leonard Adleman perfected public key cryptography or what we call RSA.



Receiver

- 1. First, the receiver picks 2 very large primes, p and q. Also, compute $n = pq$.
- 2. Compute $m = lcm(p-1, q-1)$.
- 3. Pick an e relatively prime to m.
- 4, Find d such that $ed \mod m = 1$.
- 5. Announce n and e publicly.
  NOTE: Each p and q are 100-200 digits each and n is anywhere between 200 and 400 digits.

Example

- As the receiver, choose two primes, say 37 and 73. Compute the product, which is 2701.
- Compute the lcm of 36 and 72, which is 72.
- Choose an e relatively prime to 72, say 7.
- Find a d such that $7d \mod 72 = 1$. Thus, $d = 31$.

Sender

- 1. Convert the message to a string of digits.
- 2. Break up the message into uniform blocks of digits; call them $M_1, M_2, ..., M_k$.
- 3. Calculate and send $R_i = M_i^e \mod n$.

Example

Suppose I want to send the message "YES"

- As the sender, convert the letters into a string of digits. Use a code for each of the 26 letters starting with a=01 through z=26 and blank with 00.
- We have 250519.
- Now, break these up into strings of length 4. This gives strings $M_1 = 2505, M_2 = 1900$.
- Compute $R_1 = 2505^7 \mod 2701 = 692$, $R_2 = 1900^7 \mod 2701 = 1734$.
- The sender will send 0692 and 1734.

Receiver

- 1. For each received message, R_i, calculate $R_i^d \mod n$.
- 2. Convert the string of digits back to a string of characters.

Example

- 0692 and 1734 will be received.
- As the receiver, now compute $692^{31} \mod 2701 = 2505$ and $1734^{31} \mod 2701 = 1900$.
- Now convert 25051900 back to letters to decrypt the message.
- We know each letter is encoded with a two-digit number.
- Split 25051900 into blocks of 2.
- This gives 25 (Y), 05 (E), 19 (S).

Mod Simplification

- Consider 692^{31}. If we were to compute this, we get a number 89 digits long.
- Take $692^{31} = (692^2)^8(692^3)^5$. The numbers are much smaller and easier to deal with.
- $692^{31} \mod 2701 \equiv ((692^2 \mod 2701)^8 \mod 2701) \cdot ((692^3 \mod 2701)^5 \mod 2701) \mod 2701$
- We only have 692^2 and 692^3, which are 6 and 9 digits, instead of 89.
- Now, to mod out by 2701, the problem is quicker by far.

Proof

Fermat's Little Theorem

If p is any prime number, and a is any integer such that $p \nmid a$, then $a^{p-1} \equiv 1 \mod p$.

Chinese Remainder Theorem

A system of linear congruences modulo pairwise relatively prime integers has a unique solution modulo the product of these moduli.

Proof

- Assume $de \equiv 1 \mod (p-1)(q-1)$. Then, there exists an integer, k, such that $de = 1 + k(p-1)(q-1)$.
- It follows that $R^d \equiv (M^e)^d = M^{de} = M^{1+k(p-1)(q-1)} \mod n$.
- $gcd(M,p) = gcd(M,q) = 1 \Rightarrow M^{p-1} \equiv 1 \mod p$ and $M^{q-1} \equiv 1 \mod q$.
- Therefore, $R^d \equiv M \cdot (M^{p-1})^{k(q-1)} \equiv M \cdot 1 = M \mod p$
- Also, $R^d \equiv M \cdot (M^{q-1})^{k(p-1)} \equiv M \cdot 1 = M \mod q$
- $gcd(p,q) = 1 \Rightarrow R^d \equiv M \mod pq$.

Future Work

- RSA can fuel more research around prime numbers.
- That being said, if someone figures out a way to factor large numbers into two primes rather quickly, security will be compromised.
- Some non-secret forms of communication, such as email, can be used between the sender and receiver to speed up the process since the RSA process is time consuming.
- Until 2007, RSA gave cash prizes for factoring large numbers into two primes.

References

K. H. Rosen,
Discrete Mathematics and Its Applications 7th Edition,
Monmouth University, 2007.

S. Epp,
Discrete Mathematics with Applications 4th Edition,
Brooks/Cole, 2011.

Public Key Cryptography: RSA Encryption Algorithm,
https://www.youtube.com/watch?v=wXB-V_Keiu8
Princeton University Press, 2008.

- Thanks to Professor Beagley for advising me on this project!
- Thanks to you all for being here!
- For any further questions or comments, email me at seth.hamilton@valpo.edu.