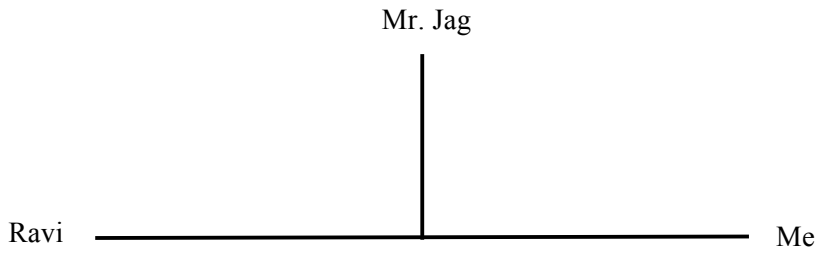
Taeyoung Kim
003711-0016
IB Mathematics HL
Exploration

RSA Encryption

RSA encryption is a public key cryptography algorithm that uses prime factorization as the trapdoor one-way function. One-way function is easy to compute in one direction, but it gets difficult to reverse unless you have the special information, the trapdoor in this case. It is easy to encrypt a message in one way, but it is extremely difficult to decrypt without the trapdoor. This asymmetric system is based on the time complexity and difficulty of factoring the products of two large prime numbers. This topic is intriguing to me because RSA encryption is most widely used cryptosystem in the world; every user on the Internet uses it, but most of us do not know how it actually works.

To apply the RSA encryption into our daily lives to see how it works, I propose a situation that may or may not be true.

My friend Ravi and I can neither confirm nor deny that we are currently attempting to plan our senior prank. Hypothetically speaking, in order to initiate the planning process, we would have to pick a date. However, Mr. Jag, the IT Director who oversees the school facilities, would do his best to prevent this event from happening. He is capable of listening to our conversation and monitoring the school network. In such situation, Ravi and I would try to be as discrete as possible, so Mr. Jag doesn't find out the date and ruin it. We would use RSA encryption to communicate the set date.



Communication Map 1

The *Communication Maps* will show the transactions of messages between the three of us throughout this paper.

First, Ravi would pick any two close prime numbers, 53 and 59, then find the n.

$$P_1 = 53, P_2 = 59$$

$$\text{n} = 53 \times 59 = 3127$$

Now, Ravi needs to use *Euler's totient function,* also known as Phi(ϕ) function in order to proceed. Phi function is defined as the number of positive integers $\leq$ n that are relatively prime[1] n, where 1 is counted as being relatively prime to all numbers[2]. Given number n, $\phi(\text{n})$ outputs how many integers are less than or equal to n, that do not share any factors with n.

Phi function of a prime number has a special characteristic. Since prime number does not have factors greater than one, the Phi of any prime number p, $\phi(\text{p}) = p - 1$. For example, $\phi(7) = 6$, since none of the number from 1 to 6 shares a factor with 7.

[1] do not contain any factor in common with
[2] Totient Function

Ravi can easily find the $\phi(n)$, because Phi function is also multiplicative when a and b are relatively prime. Meaning, $\phi(A \times B) = \phi(A) \times \phi(B)$.

If n is a product of two prime numbers, $n = P_1 \times P_2$

$$\phi(n) = \phi(P_1) \times \phi(P_2)$$

$$\phi(n) = (P_1 - 1) \times (P_2 - 1)$$

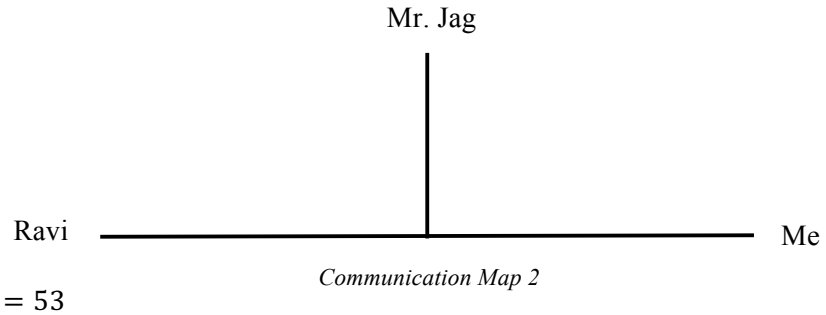
Since his numbers, 53 and 59, are relatively prime (because they have no common factor), Ravi can utilize this property.

$$n = 53 \times 59 = 3127$$

$$\therefore \phi(n) = \phi(53 \times 59) = \phi(53) \times \phi(59)$$

$$\phi(3127) = (53 - 1) \times (59 - 1) = 3016$$

So far, Ravi has the following variables:



Communication Map 2

$P_1 = 53$
$P_2 = 59$
$n = 3127$
$\phi(n) = 3016$

Now, Ravi picks a random small public exponent, e, which satisfies the following conditions:

$\cdot\ 1 < e < \phi(n)$

$\cdot$ e must be an odd number

$\cdot$ e and $\phi(n)$ *are* coprimes, meaning that e does not share a factor with $\phi(n)$

Ravi chooses 17 for the value of e, which is reasonable and satisfies all the conditions.

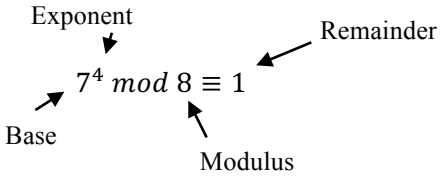
$$e = 17$$

RSA encryption utilizes modular arithmetic, which is the arithmetic of congruence. In modular arithmetic, numbers "wrap around" upon reaching a given fixed quantity, which is known as the modulus[3].

For a positive integer n, two integers m and a are said to be congruent modulo n, written:

$$\mathrm{m} \equiv \mathrm{a} \pmod{\mathrm{n}}$$

Generally, we take a number, raise it to some exponent, divide it by the modular and output the remainder. For example, when $m = 7\ and\ n = 8$,



$$2401 \bmod 8 \equiv 1$$

When m, 7, is raised to the power of Phi of n, or in this case, 4, and divide by n, 8, the remainder will be always 1.

Now Ravi would need to manipulate Euler's Theorem, which shows the relationship between the Phi function and modular exponentiation, also known as clock arithmetic. This will finalize the encryption process. Euler's Theorem states that:

$$m^{\phi(\mathrm{n})} \equiv 1 \bmod n$$

Ravi could modify the equation using two simple properties. First, when 1 is raised to any exponents, k the result is always one.

$$1^k = 1$$

In the same way, Ravi could multiply the exponents $\phi(\mathrm{n})$ by any numberk, and the result is still 1.

$$m^{\mathrm{k}\times\phi(\mathrm{n})} \equiv 1\ mod\ n$$

Secondly, if Ravi multiply one to any number such as m, it always equals m.

$$1 \times \mathrm{m} = \mathrm{m}$$

With this property, Ravi could modify the left side of the equation by m to get m on the right side.

$$m \times m^{\mathrm{k}\times\phi(\mathrm{n})} \equiv m\ mod\ n$$

The equation can be simplified as:

[3] Modular Arithmetic

$$m^{\mathrm{k}\times\phi(\mathrm{n})+1} \equiv m \bmod n$$

Now Ravi has arrived at the point where he has the equation for finding e and d, the encryption key and the decryption key respectively.

$$m^{\mathrm{e}\times\mathrm{d}} \equiv m \bmod n$$

Now he can calculate $e \times d$, which depends on $\phi(\mathrm{n})$.

$$\mathrm{e}\times\mathrm{d} = \mathrm{k}\times\phi(\mathrm{n}) + 1$$

$$\therefore d = \frac{\mathrm{k}\times\phi(\mathrm{n}) + 1}{e}$$

Because RSA cryptosystem has two separate keys, it is easy to process d only if the factorization of n is known.

However we cannot calculate d, without knowing the value of k. Also k cannot be found unless we know d. Therefore, Ravi needs to use different method to find d.

Because d is multiplicative inverse of e $(\mathrm{mod}\ \mathrm{m})$, $if\ ed \equiv 1\ (\mathrm{mod}\ m)$, Ravi can put the equation as follow:

$$d \equiv e^{-1} (\mathrm{mod}\ \phi(\mathrm{n}))$$

In this case, $\mathrm{d} \equiv 17^{-1} (\mathrm{mod}\ 3016)$

Ravi must find the multiplicative inverse of 17 mod 3016 in order to calculate d. He can do so by relating it to Euclidean Algorithm for finding GCD.

$\mathbf{3016} = \mathbf{17}(177) + \mathbf{7}$	$7 = 3016 - 17(177)$
$\mathbf{17} = \mathbf{7}(2) + \mathbf{3}$	$3 = 17 - 7(2)$
$\mathbf{7} = \mathbf{3}(2) + \mathbf{1}$	$1 = 7 - 3(2)$

Euclidean Algorithm is performed on the left column. It will verify that *gcd*(17, 3016) = 1. The right column shows the solving for the remainders.

In cases like this where *gcd*(a, b) = 1, the integer equation reads

$$1 = \mathrm{ax} + \mathrm{by}$$

$$\therefore 1 \equiv b\mathrm{y} \bmod \mathrm{a}$$

In this case,

$$1 = 17x + 3016y,$$

Ravi would now reverse the process using the equations on the right and substitute starting with that last equation and working backwards and combine terms:

$1 = 7 - 3(1)$

$1 = 7 - (17 - 7(2))(2)$

$1 = 3016 - 17(177) - (17 - (3016 - 17))(2))(2)$

$1 = 3016 - 17(177) - (17 - (3016(2) - 17((354)))(2)$

$1 = 3016 - 17(177) - (17(355) - 3016(2))(2)$

$1 = 3016 - 17(177) - (17(710) - 3016(4))$

$1 = 3016(5) - 17(877)$

$1 = 17(-887) + 3016(5)$

$17^{-1} = -887 = 2129$

In terms of residue value for multiplicative inverse,

$$1 \equiv 17(2129) \bmod 3016$$

$$\therefore d = 2129$$

d is the trapdoor that will undo the effect of e.

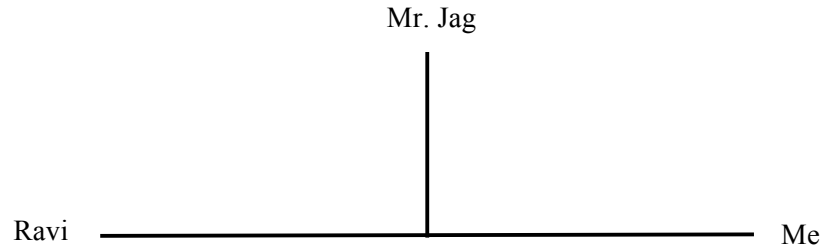
Ravi can find the value of k for the future reference.

$$\mathrm{k} = \frac{(e \times d) - 1}{\phi(\mathrm{n})}$$

$$\therefore \mathrm{k} = \frac{(17 \times 2129) - 1}{3016} = 12$$

And with the k value, Ravi can calculate d using the following formula: $d = \frac{\mathrm{k} \times \phi(\mathrm{n}) + 1}{e}$, and the result yields the same value of 2129.

Now Ravi has:

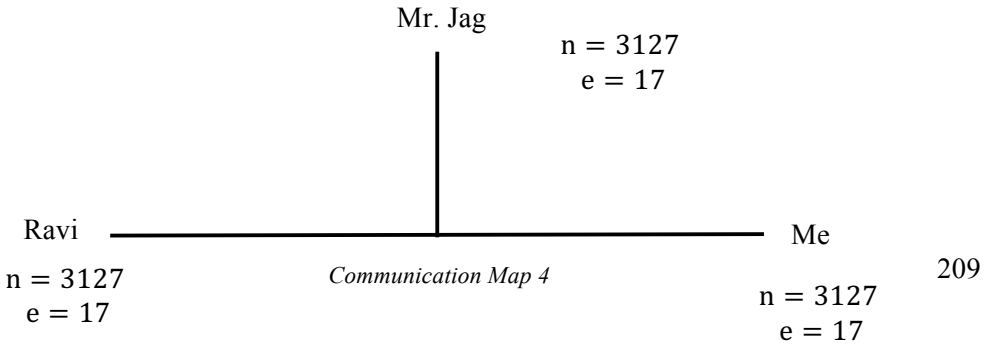


Communication Map 3

$P_1 = 53$
$P_2 = 59$
$n = 3127$
$\phi(n) = 3016$
$e = 17, d = 2129$

While Ravi was calculating his public and private keys, I picked a date, February 9th, and converted it into numerical value of 209.

Then Ravi hides everything but his public keys, n and e, and send them to me. As Mr. Jag is monitoring our conversation, he also acquires Ravi's public keys.



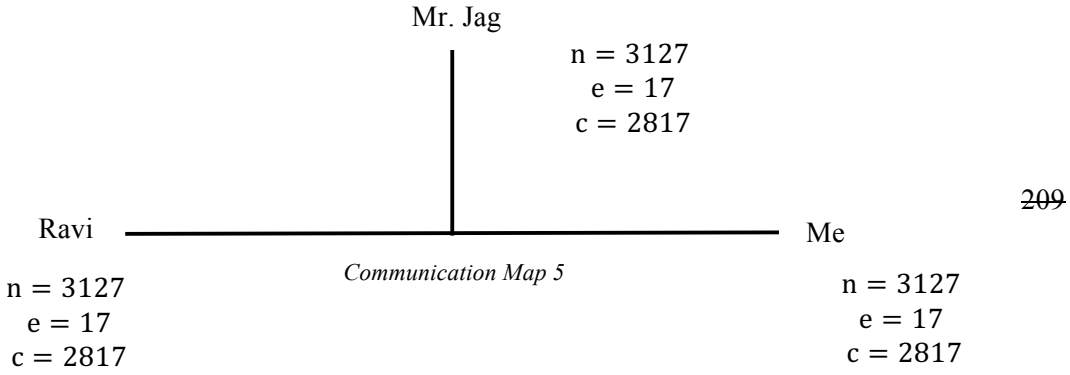
Communication Map 4

I will have to encrypt my message "209" using Ravi's public keys to securely send the message to Ravi.

With Ravi's public keys,

$$209^{17} \bmod 3127 \equiv 2817$$

$$c = 2817$$



~~209~~

Communication Map 5

Once I encrypted my message, c, would be sent to Ravi publicly, which means Mr. Jag will also receive my encrypted message.

Ravi can easily decrypt the message by accessing his trapdoor d.

$$2817^{2129} \equiv 209 \bmod 3127$$

The message of "209" was successfully received by Ravi.

Mr. Jag on the other hand, cannot crack the encrypted message due to the lack of the trapdoor. This is the most critical part of the RSA encryption, and what makes RSA so successful. With only $n, e,$ and c, Mr. Jag cannot find the trapdoor, unless he can calculate $\phi(n)$, which requires that he knows the prime factorization of n. This would normally take a massive amount of time and would require powerful computing power, but in this case, with such a small n, it would less than a second with an average personal computer. Although I doubt Mr. Jag has profound knowledge in mathematics.

Websites we use every day utilize extremely large number of n, which would require hundreds of years and the most powerful networks of computers to crack the prime factorization of n. Messages also gets encrypted, and normally, websites uses separate cryptosystems to encrypt the message, often not numerical, which makes it harder for hackers to decrypt the message without the specific trapdoors.

Bibliography

1. "Modular Arithmetic." Wolfram MathWorld. Wolfram Research, Inc., n.d. Web. 30 Jan. 2015.
2. "Totient Function." Wolfram MathWorld. Wolfram Research, Inc., n.d. Web. 28 Jan. 2015.
3. The Euclidean Algorithm and Multiplicative Inverses (2011): n. pag. The University of Utah. The University of Utah, 2011. Web. 7 Dec. 2014.
4. "Public Key Cryptography: RSA Encryption Algorithm." YouTube. Art of Problem, 30 July 2012. Web. 30 Jan. 2015.
5. "RSA Encryption." Wolfram MathWorld. Wolfram Research, Inc., n.d. Web. 30 Jan. 2015.