5-1-2010

Unbreakable Codes: RSA Public Key Cryptosystem

Razia Amzad
Pace University

Unbreakable Codes

RSA Public Key Cryptosystem

Razia Amzad

Major: Mathematics

Spring 2010

Advisor: Dr. Shamita Dutta Gupta
Professor of Mathematics
Department of Mathematics
Pace University
New York, NY 10038

Abstract

A Public Key Cryptosystem uses encoding keys that are the form of modulus m and the exponent k which can be distributed to the public while the decoding method remains secure. Public Key Cryptosystems are also known as RSA coding, which are used often because the internet runs on open networks. Public Key Cryptosystems are used with open systems mainly because there are higher risks than with older forms of e-commerce that run on closed networks such as electronic data interchange (EDI) or electronic fund transfer (EFT). Open networks create a variety of security challenges such as the integrity of the information being transmitted, the confidentiality of private or personal information, the authenticity of the communicating parties, and the assurance that the communicating parties have the authority to enter into the transactions. Public Key Cryptosystems allow secure internet transactions by providing authentication, confidentiality, digital signatures, data integrity, and non- repudiation, which prevents the receiver of a message from denying that the message had been received . Cryptography plays an essential role in protecting the privacy of electronic information against threats from a variety of potential attackers.

The purpose of this paper is to comprehend the evolution of codes and ciphers; along with understanding how to encode and decode a message using RSA coding. In this paper "Unbreakable Codes" we will highlight the historical advances of communicating secure messages, by illustrating the process of RSA coding with an example.

Table of Contents

List of Figures and Tables

Introduction

Throughout history civilizations have needed encryption to transmit messages. From Ancient Greeks to the present, we still find it necessary to send protected messages. In today's society we use encryption more than ever. Which is mainly due to the openness of the internet, currently we need encryption to protect ourselves from identity thief.

Codes and ciphers have been used since ancient times. The word cryptography, meaning the science of codes, comes from the Greek words kryptos (secret) and graphos (writing).A code can be a common phrase, which may consist of one or more letters, numbers, or words, are replaced by, four or five letters or numbers, called a code group. A cipher system or cryptographic system is any system which can be used to change the text of a message with the aim of making it unintelligible to anyone other than intended recipients. Breaking a code can be extremely complex and long without a cipher.

Ancient Greeks and Romans were the earliest civilization to use ciphers and codes. One of the oldest categories of ciphers is shorthand, which was developed by the Greeks by the fourth century BC. This code was effective and in use for 600 years until Emperor Justinian forbade its use in the year 534AD, no other system of short hand has been used for such an extensive time period (**[5]** Haldane p35). The first clear record of an enciphered message goes back to the year 405 BC during the Peloponnesian War. The general Lysander of Sparta was sent a coded message written on the inside of a servant's belt. When Lysander wound the belt around a wooden baton the message was revealed. The message warned Lysander that Persia was about to go to war against him. He immediately set sail and defeated the Persians. Another example of a cipher was developed in Greece by Polybius, who created a system of signaling, using a combination of letters and numerals, it was used as the basis of a German cipher ADFGX during WWI. To indicate letters, the numeral at the left hand side was written first followed by the one on top, for example R would be written as 42 and A as 11. This can be seen below.

Fig. 1 *Polybius Square*

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Julius Caesar created his own cipher; where he moved each letter of the alphabet along three places. Julius Caesar's cipher is not a sophisticated method, since it reveals the amount of letters and words in the message. This cipher is called a simple substitution cipher where the normal alphabet is replaced by a permutation of itself. Each letter of the normal alphabet is replaced, whenever it occurs, by the letter that occupies the same position in the permutated alphabet. This form of

cipher is commonly used in children toys, where children get a secret message and have to wait to get a decoder ring to find out the secret message. A simple cipher, can be broken by making a frequency count of the letters, attempt to identify the spaces and then attempt to identify the cipher representations of some high frequency letters like **E,T,A,I,N** and **O** which together typically amount for over 40% of the entire text, with E being the most common used letter. Next, with some parts of words identified look for short words with one or two letters still unknown. Finally, complete the solution by using grammatical and contextual information (**[1]**Churchhouse p17-19). Code-breakers can begin to speculate at the meanings by studying mathematical calculation to crack a code. A code-breaker can be assisted by the capture of a cipher, like an enemy codebook, or by mistakes made by the person sending the message. Once a code has been broken and a cipher has been found, other messages sent in that code can easily be deciphered.

Another form of cipher is a two letter cipher which is an encryption system where a plaintext letter becomes more than one letter in the cipher and there are also other systems in which encipher the text two (or more) letters at a time. The first type is a monograph to digraph, where the alphabet is written on a 5 X 5 square with one letter omitted. The omitted letter is usually **J**, which is replaced **I**, if required. The five rows and columns of the square are **A, B, C, D** and **E,** an example of this can be seen below. Each plaintext letter is now replaced by its row and column letters, so for instance **R** becomes **DB**. This cipher is pretty weak but it can become more secure by shuffling the alphabet inside the 5 X 5 box (**[1]** Churchhouse p54-55).

Fig. 2 *Two Letter Cipher*

	A	B	C	D	E
A	A	B	C	D	E
B	F	G	H	I/J	K
C	L	M	N	O	P
D	Q	R	S	T	U
E	V	W	X	Y	Z

In stencil ciphers certain letters on a page are part of the secret message and all the other letters are merely fillers which are used to compose a mundane looking communication. An appropriate stencil would use letters that are separated from each other by irregular intervals and which are not necessarily the first letters of words. For added security the letters in the secret text would probably not occur in the correct order in the overall text. In order for a recipient to be able to decode the message the sender would have to have a regular format where the cards have holes punched in them at the positions of the letter of the secret message.

"During the 1914-1918 war radio began to be used by military units for sending messages to each other and to their headquarters" (**[1]** Churchhouse p 111). Radio allowed communication between units along great distance almost immediately but the downfall of radio is that it allowed the enemy to intercept the message. After the war a number of people across the world tried to create a machine that was able to encode and decode messages. In the early 1920's a German engineer, Arthur Scherbius created a number of cipher machines, which were created to provide a large number of alphabet substitutions. "A different alphabet would automatically be used every time a

letter was enciphered, and no substitution alphabet would reoccur until thousands of letters had been processed" (**[1]** Churchhouse p111). Once Scherbius decided on his design he called it Enigma. The Enigma machine looked like a typewriter in a wooden box. An electric current went from the keyboard through a set of rotors and a plug board to light up the 'code' alphabet. Enigma could put a message into code in over 10^{17} different variations. Germans believed that no one could crack the Enigma code; At least once a day Germans altered the order of the rotors, their starting positions and the plug board connections. To decipher a message sent using Enigma, one had to work out exactly how all of these had been set. During the 1930's Polish cipher experts secretly began to try to crack the code. Just before the war, they managed to pass models and drawings of Enigma to British and French code-breakers (**[7]** Enigma and Codes).

Electronic Data Interchange (EDI)has been around since the late 1960s it is used to transfer electronic documents from one computer system to another; transactions take place between computers or databases, not individuals. Two elements of EDI are that "electronic documents replace paper based ones and the exchange of documents takes place in a standardized format" (GXS). The paper documents that Electronic Data Interchange can take the place of purchase orders, invoices, health insurance claims, and shipping notices. "While rare, the possibility that data will be intercepted and stolen or altered in transit does exist. Messages also may be deliberately or mistakenly duplicated. This can result in overcharges, wasted resources, and damaged relations between trading partners" (**[2]**Electronic Data Interchange (EDI) - Security Issues.)

Electronic Fund Transfer (EFT) is a computer based system used to perform financial transactions electronically. It is used for direct deposit, cardholder-initiated transactions, and online banking. Through illegally altering payment instructions in the EFT process, an individual could steal a large amount of money. "Although it is difficult, if not impossible, to obtain accurate statistics on EFT fraud, one could suggest that companies lose huge sums each year due to fraudulent EFT payment instructions" (**[6]** Humphries).

Codes and ciphers grow increasingly more complex, mainly because people have found cracks in previous forms of codes. Due to this risk people have found it necessary to develop more complex methods to create an unbreakable code that will safely store their information from others.

RSA Encryption

The RSA public key cryptosystem is named after its three inventors Ron Rivest, Adi Shamir, and Leonard Adleman. The name public key reflects that the encoding key consisting of modulus m and the exponent k can be distributed to the public while the decoding method remains secure. The concept of the having a code where knowledge of the encoding process does not enable one to decode a message was brought forward by Whitfield Diffie and Martin Hellman in 1976. By 1977 Ron Rivest, Adi Shamir, and Leonard Adleman created the RSA public key cryptosystem. The RSA public key cryptosystem is based on the belief that it is extremely difficult to factor large composite integers. RSA Coding has survived all forms of attack since August 1977. RSA coding is not extremely fast but it is definitely secure; since 1977, the world's best mathematicians who have access to any form of computing power have failed to attack the RSA system. Due to the length of time RSA coding has remained secure it is currently accepted as a worldwide standard (**[3]**Flannery).

The cipher text of the RSA procedure is a one-way function of the plaintext. Meaning that "transitions from one number to another are easy in one direction and difficult in the opposite direction" (**[8]**Kippenhahn 243). The reason that RSA coding is a one-way function is due to the fact that multiplying two large prime numbers by each other is relatively simple, but it is virtually impossible to factor such a number into its elements. Once someone is able to find the two prime elements of the large number the code is cracked. However, there is no simple way to factor a number that is more than a hundred digits long other than trial and error. Therefore, if one wanted to crack an RSA code he or she would have to take the public key and divide by prime numbers starting at two until there is he finds one that does not have a remainder; but with a large prime numbers this can take forever. According to Ron Rivest, Adi Shamir, and Leonard Adleman "one would have to perform some 14 billion mathematical steps in order to factor a five digit number… even though computers have become faster, a 500 digit number requires a forty digit number of mathematical operations-too much for even the most modern computers"(**[8]**Kippenhahn 230). RSA encryption is efficient because it does matter whether an encryption can be cracked but whether it can be cracked quickly.

"The RSA algorithm is the most widely used method of implementing public key cryptography and has been deployed in more than one billion applications worldwide"(**[8]**RSA Security).RSA encryption is currently used in authentication, access control, credential management, data loss prevention, fraud prevention, encryption , key management, and information security.

Definitions, Theorems, and Proofs

Euclidean Algorithm:

To compute the greatest common divisor of two numbers a and b, let $r_{-1} = a$, let $r_0 = b$, and compute successive quotients and remainders

$$r_{i-1} = q_{i+1} \times r_i + r_{i+1}.$$

For $i = 0,1,2, \ldots$ until some remainder r_{n+1} is 0. The last nonzero remainder r_n is the greatest common divisor of a and b.

Proof:

Each time we compute a quotient with remainder,

$$A = Q \times B + R,$$

the remainder will be between 0 and $B - 1$. Since $R \geq B$, then we can add one more onto the quotient Q and subtract B from R. So the successive remainders in the Euclidean algorithm continually decrease:

$$b = r_0 > r_1 > r_2 > r_{3\ldots}$$

All the remainders are greater than or equal to 0, so we have a strictly decreasing sequence of nonnegative integers. Eventually, we must reach a remainder that equals 0; we will reach 0 in at most b steps.

Linear Equation Theorem:

Let a and b be nonzero integers and let g= gcd (a, b). The equation

$$ax + by = g$$

always has a solution (x_1, y_1) in integers and this solution can be found by the Euclidean algorithm. Then every solution to the equation can be obtained by substituting integers k into the formula

$$(x_1 + k \cdot \frac{b}{g}, y_1 - k \cdot \frac{a}{g}).$$

Proof:

Take a and b are relatively prime, $\gcd(a, b) = 1$ and suppose the (x, y) is a solution to the equation

$$ax + by = 1$$

We can create additional solutions by subtracting a multiple of b from x_1 and adding the same multiple of a onto y_1.

For any integer k we obtain a new solution$(x_1 + kb, y_1 - ka)$. We can check by computing

$$a(x_1 + kb) + b(y_1 - ka) = ax_1 + akb + by_1 - bka = ax_1 + by_1 = 1$$

Looking at $\gcd(a, b) = 1$, we can show that gives all possible solutions.

Suppose that we are given two solutions (x_1, y_1) and (x_2, y_2) to the equation $ax + by = 1$.

$$ax_1 + by_1 = 1 \quad \text{and} \quad ax_2 + by_2 = 1.$$

Multiplying the first equation by y_2, multiply the second equation by y_1 and subtract we are left with

$$ax_1 y_2 - ax_2 y_1 = y_2 - y_1$$

If we multiply the first equation by x_2 , multiply the second equation by x_1 and subtract

$$bx_2 y_1 - bx_1 y_2 = x_2 - x_1$$

So if we let $k = x_2 y_1 - x_1 y_2$ then we find that

$$x_2 = x_1 + kb \text{ and } y_2 = y_1 - ka$$

This shows that the second solution (x_2, y_2) is obtained from the first solution (x_1, y_1) by adding a multiple of b onto x_1 and subtracting the same multiple of a from y_1. Therefore every solution to $ax + by = 1$ can be obtained from the initial solution (x_1, y_1) by substituting different values of k into$(x_1 + kb, y_1 - ka)$.

If $\gcd(a, b) > 1$ Let $g = \gcd(a, b)$. We know from the Euclidean algorithm that there is at least one solution (x_1, y_1) to the equation

$$g = ax + by$$

But g divides both a and b so (x_1, y_1), is a solution to the simpler equation

$$\frac{a}{g}x + \frac{b}{g}y = 1$$

Now our earlier work applies, so we know that all other solution can be obtained by substituting values for k in the formula

$$(x_1 + k \cdot \frac{b}{g}, y_1 - k \cdot \frac{a}{g}).$$

This completes our description of the solution to the equation $g = ax + by$.

Euler's Formula

If $\gcd(a, m) = 1$ and b is relatively prime to m then

$$a^{\phi(m)} \equiv 1\ (mod\ m).$$

Proof:

Suppose the $\gcd(a, m) = 1$ then the numbers

$$b_1 a, b_2 a, b_3 a, \ldots b_{\phi(m)} a\ (mod\ m)$$

are the same as the numbers although they may be in a different order

$$b_1, b_2, b_3, \ldots b_{\phi(m)}\ (mod\ m).$$

Then the product of the numbers in the first list is equal to the product of numbers in the second list

$$(b_1 a) \cdot\ (b_2 a) \cdot\ (b_3 a) \cdots \left(b_{\phi(m)} a\right) \equiv b_1 \cdot b_2 \cdot b_3\ \cdots b_{\phi(m)} (mod\ m)$$

Let us factor out $\phi(m)$ copies of a

$$a^{\phi(m)} B \equiv B(mod\ m), \quad where\ B = b_1 \cdot b_2 \cdot b_3\ \cdots b_{\phi(m).}$$

Since each of it b_i's are relatively prime to m, B is relatively prime. Canceling B from both sides we get Euler's formula

$$a^{\phi(m)} \equiv 1\ (mod\ m).$$

Fermat's Little Theorem

Let p be a prime number, and let a be any number with $a \not\equiv 0\ (mod\ p)$. Then

$$a^{p-1} \equiv 1(mod\ p).$$

Proof:

We start by listing the first $p - 1$ positive multiples of a:

$$a, 2a, 3a, \ldots (p\ -1)a$$

Suppose that ra and sa are the same $modulo\ p$, then we have

$$r\ =\ s\ (mod\ p),$$

so the $p - 1$ multiples of a above are distinct and nonzero; that is, they must be congruent to $1, 2, 3, \ldots,\ p - 1$ in some order.

Multiply all these congruencies together and we find

$a.2a.3a.\ldots.(p-1)a\ \equiv\ 1.2.3.\ldots.(p-1)\left(mod\ p\right)$ or $a^{(p-1)}(p-1)!\ \equiv\ (p-1)!\ (mod\ p)$.

Divide both sides by $(p - 1)!$

$$a^{p-1} \equiv 1(mod\ p).$$

Phi Function Formulas

If p is a prime and $k \geq 1$, then

$$\phi\ (p^k) = p^k - p^{k-1}.$$

If gcd $(m, n) = 1$, then $\phi\ (m, n) = \phi(m)\phi(n)$.

Proof:

$$\phi(p^k) = {p_1}^{k_1-1}{p_2}^{k_2-1} \dots {p_n}^{k_n-1}\phi(p_1 p_2 \dots p_n)$$

$$\phi\ (m, n) = \phi(m)\phi(n).$$

Since $p_1 p_2 \dots p_n$ are all primes

$$\phi(p_1 p_2 \dots p_n) = \phi(p_1)\phi(p_2) \dots \phi(p_n).$$

If p is a prime, then all numbers less than p are co-prime to p, which means,

$$\phi(p) = p - 1$$

applying this we find

$$\phi(p_1 p_2 \dots p_n) = (p_1 - 1)(p_2 - 1) \dots (p_n - 1)$$

giving us

$$\phi(p^k) = (p_1 - 1){p_1}^{k_1-1}(p_2 - 1){p_2}^{k_2-1} \dots (p_n - 1){p_n}^{k_n-1}$$

Successive Squaring to Compute

Let m be a number larger than a and k, where k is larger than a

$$a^k\ (mod\ m).$$

The following steps compute the value of $a^k\ (mod\ m)$):

1. Write k as a sum of powers of 2.
   $$k \equiv u_0 + u_1 \cdot 2 + u_2 \cdot 4 + u_3 \cdot 8 + \cdots + u_r \cdot 2^r$$
   Where each u_i, is either 0 or 1. (This is called the binary expansion of k.)
2. Make a table of powers of modulo m using successive squaring.

$$\begin{aligned} a^1 &\equiv A_0\ (mod\ m) \\ a^2 \equiv (a^1)^2 &\equiv A_0^2 \equiv A_1\ (mod\ m) \\ a^4 \equiv (a^2)^2 &\equiv A_1^2 \equiv A_2 (mod\ m) \\ a^8 \equiv (a^4)^2 &\equiv A_2^2 \equiv A_3 (mod\ m) \\ &\vdots \\ a^{2r} \equiv (a^{2r-1})^2 &\equiv A_{r-1}^2 \equiv A_r (mod\ m) \end{aligned}$$

We note to compute each line of the table you only need to take the number at the end of the previous line, square it and reduce it modulo m. Also note that the table has $r + 1$ lines, where r is the highest exponent of 2 appearing in the binary expansion of k in Step 1.

3. The product
$$A_0^{u_0} \cdot A_1^{u_1} \cdot A_2^{u_2} \dots A_r^{u_r} \ (mod\ m)$$
Will be congruent to $a^k \ (mod\ m)$.
We note that all u_i's are either 0 or 1, so this number is really the product of those A_i's for which u_i equals 1.

Algorithm: How to Compute k[th] Roots Modulo m

Let b, k, and m be given integers that satisfy

$$\gcd(b, m) = 1 \text{ and } \gcd\big(k, \phi(m)\big) = 1$$

The following steps give a solution to the congruence

$$x^k \equiv b(mod\ m).$$

1. Compute $\phi(m)$
2. Find positive integers u and v that satisfy $ku - \phi(m)v = 1$
Another way to say this is that u is a positive integer satisfying $ku \equiv 1 \ \big(mod\ \phi(m)\big)$, so u is actually the inverse of k modulo $\phi(m)$.
3. Compute $b^u(mod$ m) by successive squaring. The value obtained gives the solution x.

How RSA encryption works

The first thing we do is choose two large prime numbers p and q;where both p and q have 100 or 200 digits each and we keep p and q secret. They are our private key. Next we multiply p and q together to get the modulus $m = pq$. Once we find m we can compute $\phi(m) = \phi(p)\phi(q) = (p-1)(q-1)$, then we choose a number k that is relatively prime to $\phi(m)$.

Now we publish the numbers m and k for the whole world to know, but we keep the values of p and q secret. Anyone who wants to send us a message uses the values of m and k to encode the material in the following

Encode

In order to begin to encode a message one must convert their message into a string of digits by using a cipher. Next, one looks at the number m and breaks their string of digits into numbers whose digits are less than the digits of m.So now their message is a list of numbers $a_1, a_2, \ldots a_r$. The next step is to raise each a value to the k^{th} power and then reduce the number modulus m. Meaning that in order to encode the message one must compute $a_1^k (mod\ m), a_2^k\ (mod\ m), \ldots a_r^k\ (mod\ m)$. These values form a new list of numbers $b_1, b_2, \ldots b_r$. This list is now the encoded message. The message that is sent to us is the list of numbers $b_1, b_2, \ldots b_r$.

Decode

To decode the encrypted message $b_1, b_2, \ldots b_r$, we use the published numbers m and k to obtain the numbers $a_1, a_2, \ldots a_r$.

Each b_i , is congruent to $a_i^k\ (mod\ m)$, so to find a_i , we need to solve the congruence

$$x^k \equiv b_i\ (mod\ m).$$

Since we published m we know the prime factors (p and q) of that number.

We can now compute

$$\phi(m) = \phi(p)\phi(q) = (p-1)(q-1).$$

Using successive squaring and applying the algorithm to compute k^{th} Roots Modulo m we solve each of the congruencies

$$x^k \equiv b_i\ (mod\ m).$$

To find x we use the formula

$$ku - \phi(m)v = 1$$

to find the values of u and v in order to use the u value to solve for x by using the equation $b^u (mod\ m)$

We are now able to compute $b^u (mod\ m)$ by successive squaring.

The solutions are the numbers $a_1, a_2, \ldots a_r$, and then it is easy to take this string of digits and recover the original message by using the cipher.

An Example

ENCODE

We want to encode the phrase **What's up doc?**

First we need a cipher that will replace letters with numbers

Fig.3 *Numerical Cipher*

A	11
B	12
C	13
D	14
E	15
F	16
G	17
H	18
I	19
J	20
K	21
L	22
M	23
N	24
O	25
P	26
Q	27
R	28
S	29
T	30
U	31
V	32
W	33
X	34
Y	35
Z	36

Using this as our cipher we get

Fig. 4 *Message Coded using Cipher*

W	H	A	T	S	U	P	D	O	C
33	18	11	30	29	31	26	14	25	13

Giving us 33181130293126142513

Now we begin to encode 33181130293126142513 through RSA coding

First we pick two prime numbers to represent our p and q. To make our problem easy to follow, we will choose small primes.

$$p = 3 \quad , \quad q = 7$$

To find m we need to multiplying p and q

$$m = pq$$

$$3 * 7 = 21.$$

Find $\phi(m)$

$$\phi(m) = \phi(p)\phi(q) = (p-1)(q-1)$$

$$\phi(21) = \phi(3)\phi(7) = (3-1)(7-1) = (2)(6) = 12$$

We choose $k = 5$ because (5,21)=1.

Publish

Now we publish $k = 5$ and $m = 21$ for the world to see.

Encode

Since m is two digits long we break the message into 2 digit numbers

33 18 11 30 29 31 26 14 25 13.

Next we use successive squaring and raise each number to the k^{th}power

$$33^5 = 39135393 \equiv 3 \; mod \; 21$$

$$18^5 = 1889568 \equiv 9 \; mod \; 21$$

$$11^5 = 161051 \equiv 2 \; mod \; 21$$

$$30^5 = 24300000 \equiv 18 \; mod \; 21$$

$$29^5 = 20511149 \equiv 8 \; mod \; 21$$

$$31^5 = 28629151 \equiv 19 \; mod \; 21$$

$$26^5 = 11881376 \equiv 17 \; mod \; 21$$

$$14^5 = 537824 \equiv 14 \; mod \; 21$$

$$25^5 = 9765625 \equiv 16\ mod\ 21$$

$$13^5 = 371293 \equiv 13\ mod\ 21.$$

So our code is now 3,9,2,18,8,19,17,14,16,13.

DECODE

Given the code 3,9,2,18,8,19,17,14,16,13 and $k = 5$ and $m = 21$.

Since we know m is the product of two prime numbers 3 and 7 we find $\phi(m) = 12$.

Now $ku - \phi(m)v = 1$

We have $k = 5$ $\phi(m) = 12$

Therefore $5u - 12v = 1$

Thus $u = 5$ $v = 2$

we now compute $b^5(mod\ m)$ by successive squaring . The value obtained gives the solution x.

Knowing this we can now begin to decode our message. Now we are looking for numbers between 11 and 36 so that it corresponds with our cipher

$$b^{\,u} mod\ m$$

$$m = 21\ \ u = 5\,.$$

Now we will demonstrate the method of successive squaring therefore, the first number we need to decode is 3.

$$\underline{b = 3}$$

$$3^1 \equiv 3\ (mod\ 21)$$

$$3^2 \equiv 9\ (\ mod\ 21)$$

$$3^4 \equiv\ 18\ (mod\ 21)$$

$$18 * 3 = 54$$

$$33 \equiv 54\ (mod\ 21)$$

Now we continue this process with all of the numbers in our code .

Next $\underline{\ b = 9}$

$$9^1 \equiv 9 \ (mod\ 21)$$

$$9^2 \equiv 81 \ (mod\ 21)$$

$$9^4 \equiv 6561 (mod\ 21) \ \equiv 9 \ (mod\ 21)$$

$$9 * 9 = 81$$

$$81 \ \equiv 18 \ (mod\ 21)$$

When $\underline{b = 2}$

$$2^1 \equiv 2 \ (mod\ 21)$$

$$2^2 \equiv 4 \ (mod\ 21)$$

$$2^4 \equiv 16 \ (mod\ 21)$$

$$2 * 16 = 32$$

$$32 \ \equiv 11 (mod\ 21)$$

When $\underline{b = 18}$

$$18^1 \equiv 18 \ (mod\ 21)$$

$$18^2 \equiv 324 \equiv 18 \ (mod\ 21)$$

$$18^4 \equiv 104976 \equiv 18 (mod\ 21)$$

$$18 * 18 = 324$$

$$324 \ \equiv 30 (mod\ 21)$$

When $\underline{b = 8}$

$$8^1 \equiv 8 \ (mod\ 21)$$

$$8^2 \equiv 64 \ (mod\ 21)$$

$$8^4 \equiv 4096 \equiv 1 \ (mod\ 21)$$

$$8 * 1 = 8$$

$$8 \ \equiv 29 \ (mod\ 21)$$

When $\underline{b = 19}$

$19^1 \equiv 19(mod\ 21)$

$19^2 \equiv 361(mod\ 21)$

$19^4 \equiv 130321 \equiv 16(mod\ 21)$

$19 * 16 = 304$

$304 \equiv 31(mod\ 21)$

When $\underline{b = 17}$

$17^1 \equiv 17(mod\ 21)$

$17^2 \equiv 289(mod\ 21)$

$17^4 \equiv 83521 \equiv 4(mod\ 21)$

$17 * 4 = 68$

$68 \equiv 26(mod\ 21)$

When $\underline{b = 14}$

$14^1 \equiv 14(mod\ 21)$

$14^2 \equiv 196\ (mod\ 21)$

$14^4 \equiv 38416 \equiv 7(mod\ 21)$

$14 * 7 = 98$

$98 \equiv 14(mod\ 21)$

When $\underline{b = 16}$

$16^1 \equiv 16\ (mod\ 21)$

$16^2 \equiv 256\ (mod\ 21)$

$16^4 \equiv 65536 \equiv 16\ (mod\ 21)$

$16 * 16 = 256$

$$256 \equiv 25(mod\ 21)$$

When $\underline{b = 13}$

$$13^1 \equiv 13\ (mod\ 21)$$

$$13^4 \equiv 1\ (mod\ 21)$$

$$13 * 1 = 13$$

$$13 \equiv 13\ (mod\ 21)$$

Now we get the numbers

33 18 11 30 29 31 26 14 25 13.

Using Fig. 4 *Message Coded using Cipher on pg 16*

We get

W	H	A	T	S	U	P	D	O	C
33	18	11	30	29	31	26	14	25	13

Giving us: What's Up Doc?

Conclusion

Cryptosystems become more and more complex mainly because users and developers have found that a particular system has a weakness that can be extremely fatal outcome. Due to this risk people have found it necessary to develop more complex methods to create an unbreakable code that will safely store their information from others. Currently RSA public key encryption is the most widely used method of public key cryptography and is used in authentication, access control, credential management, data loss prevention, fraud prevention, encryption, key management, and information security across the world.

References

[1] Churchhouse, R. F. *Codes and Ciphers Julius Caesar, the Enigma, and the Internet*. New York: Cambridge UP, 2001. Print.

[2] "Electronic Data Interchange (EDI) - Security Issues." *Free Encyclopedia of Ecommerce*. Web. 24 Jan. 2010. <http://ecommerce.hostip.info/pages/382/Electronic-Data-Interchange-EDI-SECURITY-ISSUES.html>.

[3] Flannery, Sarah, and David Flannery. *In Code A Mathematical Journey*. New York: Algonquin Books, 2002. Print.

[4] GXS. "What is EDI?" *EDI Basics - A Step-by-Step Guide to Electronic Data Interchange (EDI)*. 2010. Web. 24 Jan. 2010. <http://www.edibasics.co.uk/getting_started/gettingStarted_p1.html>.

[5] Haldane, R. A. *The Hidden Worlds*. New York: St. Martin's, 1976. Print.

[6] Humphries, John E. "Preventing EFT Fraud." *ISACA*. 2010. Web. 24 Jan. 2010. <http://www.isaca.org/Template.cfm?Section=Home&CONTENTID=16271&TEMPLATE=/ContentManagement/ContentDisplay.cfm>.

[7] "IWM - Enigma and the Code breakers." *Welcome to the Imperial War Museum*. Imperial War Museum. Web. 25 Nov. 2009. <http://www.iwm.org.uk/upload/package/10/enigma/index.htm>.

[8] Kippenhahn, Rudolph. *Code Breaking a History and Exploration*. Woodstock: Overlook Hardcover, 1999. Print.

[9] RSA Security. "Technology Innovation @ RSA, Then and Now." *RSA, The Security Division of EMC: Security Solutions for Business Acceleration*. 2010. Web. 15 Jan. 2010. <http://www.rsa.com/node.aspx?id=2760>

[10] Silverman, Joseph H. *Friendly introduction to number theory*. Upper Saddle River, New Jersey: Pearson Prentice Hall, 2006. Print.