Mathematics behind Cryptosystems

Rohit Rawat
App No: MATS795-I

Guide Name: Professor B.Sury

Signature of student   Signature of Guide

(Rohit Rawat)   (B.Sury)

Contents

Introduction

We study cryptosystems constructed using mathematics. Imagine two people Amit and Bani who wish to share an important secret but are at a distance. If they communicate through a public medium, an eavesdropper may intercept the messages and become privy to this information. How do they communicate safely? The idea is to communicate using some kind of cipher.

The following analogy will be helpful. First, Amit locks his messages in a box, using a lock that only he and Bani know the combination to. This is known as ‘Encryption’. Then, the locked message is sent to Bani. When Bani receives the box, she opens it using the code they shared in advance. This is known as ‘Decryption’.

Cryptography begins when we abandon physical locks and use ‘ciphers’ instead as virtual locks. Ciphers allow Amit and Bani to scramble and unscramble their messages so that it would appear meaningless if Eram intercepted it. Cryptography has been around for thousands of years. It has decided wars, and is at the heart of the worldwide communication network today. The fascinating story of cryptography requires us to understand two very important topics in mathematics - number theory and field theory.

The Caesar cipher and poly-alphabetic cipher which are fairly simple simple cryptographic systems are simple to crack using frequency analysis and other methods.

These kinds of systems use a shared key which itself has to be communicated. Therefore, there is a need for a system where the key is public but still communication is safe.

An important role in public key cryptography is played by trapdoor functions. These are functions that are easy to perform in one direction but finding their inverses is not computationally feasible without additional information. This is where the idea of factorizing a very large prime number comes into play. Computationally, it is easy to calculate the product ab of two given large numbers but it is far more difficult to find the factors from the product. We shall study in detail several public key cryptosystems constructed using methods from number theory and finite fields.

1 Topics in Elementary Number Theory

The aim of this section to introduce the readers to elementary number theory concepts that would be needed in almost every step of cryptology. A basic reference is David Burton's text book ([3]).

1.1 Divisibility and the Euclidean algorithm

Divisibility. Suppose that we have two integers a and b, we say that b is divisible by a and we write $a|b$ if there exists an integer d such that $b = ad$. a is called a divisor of b. Every integer $b > 1$ has at least two positive divisors: 1 and b. A proper divisor of b is a positive divisor of b not equal to b itself. A nontrivial divisor of b is a positive divisor of b not equal to 1 or b. A prime number is a positive integer which has no positive divisors other than 1 and itself; a number is called composite if it has at least one nontrivial divisor. Some basic properties of divisibility are as follows:

1. If $a|b$ and c is any integer, then $a|bc$.
2. If $a|b$ and $b|c$, then $a|c$.
3. If $a|b$ and $a|c$, then $a|b \pm c$.

The $Fundamental\ Theorem\ of\ Arihtimetic$ states that any natural number n can be represented uniquely(except for the order of factors) as a product of prime numbers. It is conventional to write this factorization as a product of distinct primes to their respective powers. For example, $3600 = 2^4 \cdot 3^2 \cdot 5^2$. We can infer two conclusions of the above theorem which are the following properties of divisibility:

1. If a prime p divides ab, then either $p|a$ or $p|b$.
2. If $m|a$ and $n|a$ and if $g.c.d.(m, n) = 1$, then $mn|a$.

The total number of possible divisors is the product of the number of possibilities for every prime power. Like for example if a prime p has power α as its power in the factorization, then the possible ways of choosing the powers of p are $(\alpha+1)$. Hence, a number $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ has $(\alpha_1+1)\cdot(\alpha_2+1)\cdots(\alpha_r+1)$ distinct divisors. For example, 3600 has $(4+1)\cdot(2+1)\cdot(2+1) = 45$ divisors.

Given two non-zero integers a and b, the $greatestcommondivisor$ of a and b is denoted by $g.c.d.(a,b)$. It is the largest integer dividing both a and b. Another equivalent definition of $g.c.d.(a,b)$ is: it is the only positive integer d which divides a and b and any other number that divides both a and b also divides d. It is very easy to find the $g.c.d.(a,b)$ if we have the prime factorization of two numbers. For example, comparing the factorization of $3600 = 2^4 \cdot 3^2 \cdot 5^2$ with the factorization of $4200 = 2^3 \cdot 3 \cdot 5^2 \cdot 7$, we can see that $gcd(3600, 4200) = 2^3 \cdot 3 \cdot 5^2 = 600$. Another method to find the $g.c.d.$ is using the $leastcommonmultiple$, denoted by $l.c.m.(a,b)$, which is the smallest positive integer that both a and b divide. And the $g.c.d.(a,b)$ is equal to $|ab|$ divided by $l.c.m.(a,b)$.

The Euclidean algorithm. Finding the prime factorization of very large numbers is a tedious job as we need to keep on checking one by one all the primes from 2 to $n/2$ where n is that large number. So, we need to look for quicker ways of factoring large numbers. The $Euclideanalgorithm$ is one such method where there is no such prerequisite of knowing the prime factors of a or b.

The algorithm is as follows. In order to find the $g.c.d.(a,b)$, where $a > b$, we first divide b into a and write down the quotient q_1 and the remainder r_1 as: $a = q_1 b + r_1$. Next, we perform a second division with b replacing the role of a and r_1 taking the place of b: $b = q_2 r_1 + r_2$. Again we divide r_2 into r_1: $r_1 = q_3 r_2 + r_3$. We continue doing this way until we finally obtain a remainder that divides the previous remainder. That non-zero remainder is the greatest common divisor of a and b.

Example 1. Find $g.c.d.(7854, 4746)$.

Solution.

$$7854 = 1 \cdot 4746 + 3108$$

$$4746 = 1 \cdot 3108 + 1638$$

$$3108 = 1 \cdot 1638 + 1470$$

$$1638 = 1 \cdot 1470 + 168$$

$$1470 = 8 \cdot 168 + 126$$

$$168 = 1 \cdot 126 + 42.$$

Here $42|126$, so we are done. $g.c.d.(7854, 4746) = 42$.

1.2 Congruences

Basic Properties. Let m be a positive integer. If a and b are integers such that $a - b$ is divisible by m, then we say that a and b are *congruent modulo* m, and we write

$$a \equiv b \, (mod \, m)$$

For example, $-12 \equiv 43 \, (mod \, 5)$ and $-12 \equiv 43 \, (mod \, 11)$. Two integers a and b are called *incongruent modulo* m if they are not congruent modulo m. For example, $-12 \not\equiv 43 (mod 7)$. The following properties can be directly inferred from the definition of congruency:

1. Congruence modulo m is an equivalence relation, since we can show for all integers a,b and c that:

   (a) Reflexivity: $a \equiv a \, (mod \, m)$

   (b) Symmetry: If $a \equiv b \, (mod \, m)$, then $b \equiv a \, (mod \, m)$

   (c) Transitivity: If $a \equiv b \, (mod \, m)$ and $b \equiv c \, (mod \, m)$, then $a \equiv c \, (mod \, m)$

2. For a fixed number m, each $equivalenceclass$ with respect to congruence modulo m, has exactly one representative between 0 and $m - 1$. The equivalence class of an integer a under this relation is called the *congruence class* of a modulo m. The set of equivalence classes(also called *residue classes*) will be denoted by $\mathbf{Z}/m\mathbf{Z}$. And the set of representatives for the residue classes is called a $complete \; set \; of \; residues \; modulo \; m$.

3. Congruences defined under the same modulus can be added, subtracted or multiplied. The set of equivalence classes $\mathbf{Z}/m\mathbf{Z}$ is a commutative ring, i.e. residue classes can be added, subtracted or multiplied and the result does not depend upon which representatives of the equivalence classes were used. If $a \equiv b(modm)$ and $c \equiv d \, (mod \, m)$, then $a \pm c \equiv b \pm d \, (mod \, m)$ and $ac \equiv bd \, (mod \, m)$.

4. If $d|m$ and $a \equiv b \, (mod \, m)$, then $a \equiv b \, (mod \, d)$.

5. If m and n are relatively prime i.e. $g.c.d.(m, n) = 1$, $a \equiv b \, (mod \; m)$ and $a \equiv b \, (mod \, n)$, then we have $a \equiv b \, (mod \, mn)$

Proposition 1. *The elements of* $\mathbf{Z}/m\mathbf{Z}$ *which have multiplicative inverse are those which are relativity prime to m, i.e. the numbers for which there exists b with* $ab \equiv 1 \, (mod \, m)$ *and g.c.d.(a,m)=1.*

Proof. Let $g.c.d.(a, m) = d$. It is given that $ab \equiv 1 \, (mod \, m)$ which implies that $m|(ab - 1)$. As $d|m$, so $d|(ab - 1)$. Moreover as $d|a$, so it must also divide 1. Thus, $d|1$. The only possible value of d is 1. Therefore, $g.c.d.(a, m) = 1$.

Example 2. Find $27^{-1} \, mod \, 392$, i.e. find the multiplicative inverse of 27 *modulo* 392.

Solution. Here we need to find b such that $27 \cdot b \equiv 1 \, (mod \, m)$. We begin by using the Euclidean algorithm on 27 and 392.

$$392 = 27 \cdot 14 + 14$$

$$27 = 14 \cdot 1 + 13$$

$$14 = 13 \cdot 1 + 1$$

We can write the last equation as

$$14 + 13 \cdot (-1) = 1 \tag{1}$$

Similarly we can modify the first two equations as follows:

$$27 + 14 \cdot (-1) = 13 \tag{2}$$

$$392 + 27 \cdot (-14) = 14 \tag{3}$$

Now the use the value of 13 from (2) in (1), we get that

$$14 + \{27 + 14 \cdot (-1)\} \cdot (-1) = 1$$

$$14 + 27 \cdot (-1) + 14 = 1$$

$$2 \cdot (14) + 27 \cdot (-1) = 1 \tag{4}$$

Lastly we use the value of 14 from (3) in (2) and we have

$$2\{392 + 27 \cdot (-14)\} + 27 \cdot (-1) = 1$$

$$2 \cdot 392 + 27 \cdot (-28) + 27 \cdot (-1) = 1$$

$$2 \cdot 392 + 27 \cdot (-29) = 1$$

Using modulo 392 on both the sides, we get

$$27 \cdot (363) = 1$$

So, $27 \cdot 363 \equiv 1 \; (mod\, 392)$. 363 is the multiplicative inverse of 27 under modulo 392.

Proposition 2 (Fermat's Little Theorem). *Let p be a prime number. Any integer a that satisfies $a^p \equiv 1 \; (mod\, p)$, and any integer a not divisible by p satisfies $a^{p-1} \equiv 1 \; (mod\, p)$.*

Proof. First let us suppose that $p \not| a$. Our first claim is that the integers

$$0a, 1a, 2a, \cdots, (p-1)a$$

are a complete set of residues modulo p. In order to prove this assumption we, on the contrary we let two integers ia and ja to be in the same residue class, i.e. $ia \equiv ja \; (mod\, p)$. By the definition of congruency we have that $p|(i-j)a$. Since a is not divisible by p, we have that $p|(i-j)$. But i and j are both less than p, the only possible case is $i - j = 0$ or $i = j$.

We can now conclude that the integers $0a, 1a, 2a, \cdots, (p-1)a$ are nothing but a simple rearrangement of $0, 1, 2, \cdots, (p-1)$ when considered under modulo p. Thus, it follows that the product of the numbers in the first sequence is congruent modulo p to the product of the numbers in the second sequence, i.e. $a^{p-1}(p-1)! \equiv (p-1)!(modp)$. Thus, $p|((p-1)!(a^{p-1}-1))$. Since, $(p-1)!$ is not divisible by p(p being prime), we get that $p|(a^{p-1}-1)$.We can write it as $a^{p-1} \equiv 1\,(mod\,p)$. Now if we multiply both sides of the above congruence by a, we get that $a^p \equiv a\,(mod\,p)$ that is in the statement of the proposition when a is not divisible by p.

Otherwise, when a is divisible by p, then the congruence $a^p \equiv a\,(mod\,p)$ is trivial, since both sides of the congruence are $\equiv 0\,(mod\,p)$. This finishes the proof.

Corollary. *If a is not divisible by p and if* $n \equiv m$ *mod (p-1), then* $a^m \equiv a^n$ *mod* p.

Proof. Let $n > m$. Since $(p-1)|(n-m)$, we have that $n = m + c(p-1)$ for some positive integer c. Then multiplying the congruence $a^{p-1} \equiv 1\,(mod\,p)$ by itself c times and then after that multiply by $a^m \equiv a^m(mod\,p)$ gives us the desired result $a^m \equiv a^n$.

Example 3. Find the last base-7 digit in $2^{1000000}$.

Solution. Let $p = 7$. Since 1000000 leaves a remainder of 4 when divided by $p-1$, we have $2^{1000000} \equiv 2^4 \equiv 16 \equiv 2\,mod\,7$, so the last base-7 digit is 2.

Proposition 3 (Chinese Remainder Theorem). *Suppose that* $m_1, m_2, \cdots, m_r$ *be pairwise relatively prime positive integers, i.e. g.c.d.*$(m_i, m_j) = 1$ *for* $i \neq j$. *Let integers* $a_1, a_2, \cdots, d_r$ *also be given. Suppose we want to solve a system of congruences to different moduli:*

$$x \equiv a_1\,(mod\,m_1)$$
$$x \equiv a_2\,(mod\,m_2)$$
$$\cdots \qquad \cdots$$
$$x \equiv a_r\,(mod\,m_r)$$

Then there exists a simultaneous solution x to the above system of congruences, and any two solutions are congruent to one another modulo $M = m_1 m_2 \cdots m_r$

Proof. Firstly we will prove the uniqueness of *modulo* M. Suppose the system of congruences given have two solutions, namely x' and x''. Let $x = x' - x''$. Then x must be congruent to 0 modulo each m_i, and hence modulo M(as $M = m_1 m_2 \cdots m_r$). Further we will show the construction of a solution x.

We start by defining $M_i = M/m_i$ as the product of all of the *moduli* except for the i-th modulus. Clearly $g.c.d.(m_i, M_i) = 1$. This is due to the fact that we already know that all the $m_i's$ are relativity prime and M_i does not have m_i in its factorization. So there exists an integer N_i(*inverse* of M_i and can be found by means of Euclidean algorithm like in Example 2) such that $M_i N_i \equiv 1(mod\,m_i)$. Now we set

$$x = \sum_{i=1}^{r} a_i M_i N_i.$$

Then for each i we can see that the terms in the sum other than the i-th term are all divisible by m_i, as $m_i|M_j$ whenever $i \neq j$. Thus, for each i we have: $x \equiv a_i M_i N_i \equiv a_i \, mod \, m_i$ as required.

Euler phi function. Euler phi function, also called Euler's totient function counts the number positive integers up to a given integer n that are relatively prime to n and is denoted to by $\phi(n)$.

Corollary. *The Euler phi-function is multiplicative, meaning that* $\phi(mn) = \phi(m)\phi(n)$ *whenever g.c.d.(m,n)=1.*

Proof. For finding the value of $\phi(mn)$, we need to count the number of integers between 0 and $mn - 1$ which have no common factors with mn. For each j in that range, let j_1 be its least nonnegative residue modulo m(i.e. $0 \leq j_1 < m$) and $j \equiv j_1(mod\, m))$ and let j_2 be its least nonnegative residue modulo n(i.e. $0 \leq j_2 < n$) and $j \equiv j_2(modn))$.Then it follows from the Chinese Remainder Theorem that for each pair j_1, j_2 there is one and only one j between 0 and $mn-1$ for which $j \equiv j_1(mod\, m)$ and $j \equiv j_2(mod\, n)$.

Notice that j has no common factor with mn if and only if it has no common factor with m, which is equivalent to j_1 having no common factor with m and j also has no common factor with n which is equivalent to j_2 having no common factor with n. Thus, the j's which we must count are in 1-to-1 correspondence with the pairs j_1, j_2 for which $0 \leq j_1 < m$, $g.c.d.(j_1, m) = 1$; $0 \leq j_2 < n$, $g.c.d.(j_2, n) = 1$.

The number of possible j_1's is $\phi(m)$ and the number of possible j_2's is $\phi(n)$. So the total number of possible pairs is $\phi(m)\phi(n)$. Hence, $\phi(mn) = \phi(m)\phi(n)$. This proves the above corollary.

Every positive integer n can be written as a product of prime powers, each of which has no common factors with the others (being prime), and using the formula for prime powers $\phi(p^\alpha) = p^\alpha(1 - \frac{1}{p})$, we can use the above corollary to infer that for $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r}$:

$$\phi(n) = p_1^{\alpha_1}\left(1 - \frac{1}{p_1}\right) \cdot p_2^{\alpha_2}\left(1 - \frac{1}{p_2}\right) \cdots p_r^{\alpha_r}\left(1 - \frac{1}{p_r}\right) = n \prod_{d|n}\left(1 - \frac{1}{p}\right).$$

2 Finite Fields

Before starting learning about finite fields we should familiarize ourselves with the basic definitions and properties of a field. Then we shall proceed with finite fields. A god reference is Patrick Morandi's text book ([2]).

What is a field? A *field* is a set **F** with a multiplication and addition operation which satisfy the familiar rules associativity and commutativity of both addition and multiplication, the distributive law, existence of an additive identity 0 and a multiplicative identity 1, additive inverses, and multiplicative inverses except 0. Some basic examples of field are as follows:

1. the field **Q** consisting of all rational numbers.

2. the field $\mathbf{R}$ of real numbers.

3. the field $\mathbf{C}$of complex numbers.

4. the finite field $\mathbf{Z}/p\mathbf{Z}$ of integers modulo a prime number p.

A *vectorspace* is defined over any field $\mathbf{F}$ by the same properties that are used to define a vector space over the real numbers. Every vector space has a *basis* and the number of elements in a basis is called its *dimension*. An *extensionfield* is a bigger field containing a field $\mathbf{F}$ and is by default a vector space over $\mathbf{F}$.

In similar fashion, we can define the *polynomialring* over any field $\mathbf{F}$. It is denoted by $\mathbf{F}[\mathbf{X}]$. It consists of all the finite powers of $\mathbf{X}$ with coefficients in $\mathbf{F}$. The addition and multiplication of polynomials in $\mathbf{F}[\mathbf{X}]$ is done in the same way as done with the polynomials over the reals.The *degree* d of a polynomial is the largest power of $\mathbf{X}$ which has nonzero coefficient; and in a *monic* polynomial the coefficient of $\mathbf{X}^d$ is 1.

Characteristic of a field. Now we define what we mean by *characteristic* of a field. If adding the multiplicative identity 1 to itself in $\mathbf{F}$ never gives 0, then we say that the field $\mathbf{F}$ has *characteristic zero*. Additionally we say that $\mathbf{F}$ in this case contains a copy of the field of the rational numbers. Otherwise, there is a prime number p such that

$$1 + 1 + \cdots + 1(p\,times) = 0$$

and p is called the characteristic of the field. And in this case $\mathbf{F}$ contains a copy of the field $\mathbf{Z}/p\mathbf{Z}$, which is called its prime field.

2.1 Finite Fields

Let $\mathbf{F}_q$ denote a field which has a finite number of q elements in it. Clearly a finite filed cannot have characteristic zero; so let p be the characteristic of $\mathbf{F}_q$. Then $\mathbf{F}_q$ contains the prime field $\mathbf{F}_p$= $\mathbf{Z}/p\mathbf{Z}$ and so is a vector space over $\mathbf{F}_p$ and is finite dimensional, being the extension of a finite dimensional field $\mathbf{F}_p$. There is a 1-to-1 correspondence between the elements of this f-dimensional vector space and the set of all the f-tuples of elements of $\mathbf{F}_p$. It follows that there must be f^p elements in $\mathbf{F}_q$, i.e. q is a power of the characteristic p.

From the above analysis we can infer that the cardinality of a finite field is always either a *prime* number or a *prime power* number. We shall prove the prove that for every prime power $q = p^f$, there is a field of q elements and it is unique. But first shall study the multiplicative order of elements in $\mathbf{F}_q^*$, the set of nonzero elements of our finite field. The *order* of a nonzero element is the least positive number that gives 1(or the identity).

Existence of multiplicative generators of finite fields. There are $q - 1$ nonzero elements in a finite field $\mathbf{F}_q$. By the definition of a finite field these elements form an abelian group with respect to multiplication. This simply means that the product of two nonzero elements is nonzero and is a element of the same field, the associative law and the commutative law hold, there is a identity element 1, and every nonzero element has an inverse. It is generally known that order of any element must divide the number of elements in the group, i.e. the order of the group. The proof of which is given below.

Proposition 1. *The order of any $a \in \boldsymbol{F}_q^*$ divides $q-1$*

Proof. Let d be the least power of a which equals 1, i.e. $a^d = 1$. The power of a here is finite and since the powers of a in the finite set $\mathbf{F}_q^*$ cannot all be distinct, so when we get $a^i = a^j$ for $j > i$, then we have $a^{j-i} = 1$ and here $d|(j-i)$. Let S=$\{1, a, a^2, ..., a^{d-1}\}$ denote the set of all the powers of a and for any $b \in \mathbf{F}_q^*$ let b**S** be the *coset* consisting of all the elements of the form ba^j. Then bS=$\{b, ba, ba^2, ..., ba^{d-1}\}$.

Next we prove that either two cosets are either identical or disjoint. Let b_1S and b_2S be two cosets and b_1a^i and b_2a^j be two elements of the cosets respectively. Let any element $b_1a^{i'}$ of b_1S can also be written in a form to be in b_2S. Like $b_1a^{i'} = b_1a^ia^{i'-i} = b_2a^{j+i'-i}$. From this we can infer that either two the cosets b_1S and b_2S are either identical or disjoint.

Each coset contains d elements. Since the union of all the cosets exhausts $\mathbf{F}_q^*$, i.e.

$$b_1S \cup b_2S \cdots b_nS = \mathbf{F}_q^*$$

This means that $\mathbf{F}_q^*$ is a disjoint union of d- element sets. Hence, $d|(q-1)$.

Alternate Proof. First we show that $a^{q-1} = 1$. To prove this, we write the product of all the nonzero elements in $\mathbf{F}_q^*$. There are $q-1$ elements in $\mathbf{F}_q^*$. If we multiply each of them by a, we get a rearrangement of the same elements because any two distinct elements remain distinct after multiplication by a. Thus, the product remains unaffected. But we have multiplied this product by a^{q-1}. Hence, $a^{q-1} = 1$.

Now let d be the order of a,i.e. the smallest positive power which gives 1. On the contrary let d does not divide $q-1$. Then we could find a smaller positive number r, let us call it the remainder when $(q-1) = bd + r$ such that $a^r = a^{q-1+bd} = 1 \cdot 1 = 1$. But this implies that r is the smallest positive number that gives number and this contradicts the minimality of d. Hence, $d|(q-1)$.

Generator of a field. A *generator* g of a finite field $\mathbf{F}_q^*$ is an element of order $q-1$ and the powers of g exhaust all the elements of the field $\mathbf{F}_q^*$.

Proposition 2 *Every finite field has a generator. If g is a generator of $\mathbf{F}_q^*$, then g^j is also a generator of the finite field if and only if $g.c.d.(j, q-1) = 1$. In particular, there are $\phi(q-1)$ distinct generators of $\mathbf{F}_q^*$.*

Proof. Suppose that $a \in \mathbf{F}_q^*$ and has order d, i.e. $a^d = 1$ and no lower power of a than d can give 1. By proposition 1 we have that d divides $q-1$. As a^d is the smallest power that gives 1, it is evident that the elements $a, a^2, \cdots, a^d = 1$ are all distinct. Our claim is that the elements of order d are exactly $\phi(d)$ values a^j for which $g.c.d.(j, d) = 1$. Firstly, since the d distinct powers of a all satisfy the equation $x^d = 1$, these are all roots of this equation. Any element of order d must be among the powers of a. However, all powers of a may not have order d. Whenever

$g.c.d.(j,d) = d' > 1$,then a^j has lower order: because $d|d'$ and $j|d'$ are integers, and we can write $(a^j)^{(d/d')} = (a^d)^{(j/d')} = 1$.

Conversely, we now show that a^j does have order d whenever $g.c.d.(j,d) = 1$. If j is prime to d, and if a^j had a smaller order d'', then $a^{d''}$ raised to either the jth or the dth power would give 1, and hence $a^{d''}$ raised to the power $g.c.d.(j,d) = 1$ gives 1. But this contradicts the fact that a is of order d and so $a^{d''} \neq 1$. Thus, a^j has order d if and only if $g.c.d.(j,d) = 1$. This means that an element of a of order d will have exactly $\phi(d)$ elements of d.

Corollary. *For every prime p, there exists an integer g such that the powers of g exhaust all nonzero residue classes modulo p.*

Example 1. Suppose we want to get all the residues *mod* 19. And we know $g.c.d.(2,19) = 1$. So we can get all the residues *mod* 19 from 1 to 18 by taking powers of 2. All the successive powers of 2 reduced *modulo* 19 are as follows: 2, 4, 8, 16, 13, 7, 14, 9, 18, 17, 15, 11, 3, 6, 12, 5, 10, 1.

Existence and Uniqueness of finite fields with prime power number of elements. The existence and uniqueness of finite fields with prime number of elements has been given already. Now we deal with the existence and uniqueness of finite fields with prime power number of elements. This is shown by proving that a finite field of $q = p^f$ elements is the splitting field of the polynomial $X^q - X$. The following proposition shows that for every prime power q there is one and (up to isomorphism) only one finite field with q elements.

Splitting Field. A splitting field of a polynomial with coefficients in a field is a smallest field extension of that field over which the polynomial splits or decomposes into linear factors.

Example 2. The splitting field of $x^2 - 2$ over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt{2})$ since the two roots $\pm\sqrt{2} \in \mathbb{Q}(\sqrt{2})$.

Lemma. $(a+b)^p) = a^p + b^p$ *in any field of characteristic p.*

Proof. We expand the binomial $(a+b)^p$ as:

$$(a+b)^p = \binom{p}{0}a^p + \binom{p}{1}a^{p-1}b^1 + \cdots + \binom{p}{p-1}a^1b^{p-1} + \binom{p}{p}b^p.$$

The middle $(p-1)$ elements will be multiples of p hence, will be zero as the characteristic of the field is p. The equation becomes

$$(a+b)^p) = a^p + b^p.$$

Proposition 3. *If $\mathbf{F}_q^*$ is a field of $q = p^f$ elements, then every element satisfies the equation $X^q - X = 0$, and $\mathbf{F}_q^*$ is precisely the set of roots of that equation. Conversely, for every prime power $q = p^f$ the splitting field over $\mathbf{F}_q^*$ of the polynomial $X^q - X$ is a field of q elements.*

Proof. First let us suppose that $\mathbf{F}_q^*$ is a finite field. By proposition 1, we have that the order of every nonzero element divides $q-1$. Thus, it follows that any nonzero element satisfies the equation $X^{q-1} = 1$, and multiplying both sides by X, the equation becomes $X^q = X$. The 0 element will definitely satisfy the given equation trivially. Thus, all q elements of $\mathbf{F}_q^*$ are roots of the degree-q polynomial $X^q - X$. This polynomial cannot have more than q roots, therefore its roots are exactly the same elements of $\mathbf{F}_q^*$. This means that $\mathbf{F}_q^*$ is the splitting field extension of the polynomial of $X^q - X$, i.e. the smallest field extension of $\mathbf{F}_p^*$, which contains all its roots.

Conversely, let $q = p^f$ be a prime power, and let $\mathbf{F}$ be the splitting field over $\mathbf{F}_p^*$ of the polynomial $X^q - X$. We want to show that this splitting field is a field of q elements. The polynomial $X^q - X$ has derivative $qX^{q-1} - 1 = -1$(because the integer q is a multiple of p and so is zero in the field $\mathbf{F}_p^*$ having characteristic p). The derivative has no roots at all. Hence, the polynomial $X^q - X$ has no root in common with its derivative, and therefore has no multiple roots. Thus, $\mathbf{F}$ contains at least the q distinct roots of the polynomial $X^q - X$. But we claim that the set of q roots is already a field. If a and b satisfy the polynomial, then the product of a and b is also a field as $a^q = a$, $b^q = b$ and hence, $(ab)^q = ab$. And to show that the sum is also a root, we use the lemma that we had proved before this proposition. Repeated application of the lemma gives us that:

$$(a+b)^p) = a^p + b^p$$

$$(a+b)^{p^2} = (a^p + b^p)^p = (a+b)^p$$

$$\dots$$

$$(a+b)^q = a^q + b^q = a + b.$$

Hence, $(a+b)$ is also a root of the polynomial $X^q - X$. And we conclude that the set of q roots is the smallest field containing the roots of $X^q - X$, i.e. the splitting field of this polynomial is a field of q elements. This completes the proof.

2.2 Explicit construction

Construction of finite fields of the form $\mathbf{F}_p$=$\mathbf{Z}/p\mathbf{F}$ is fairly easy and has been dealt with in the previous sections. We now discuss how to work with finite field extensions of $\mathbf{F}_p$. In Example 2, we had a glimpse of how an extension of a field looks like when we worked with $\mathbb{Q}(\sqrt{2})$, an extension of the field of rational numbers $\mathbb{Q}$. We get this field extension by taking a root of the equation $X^2 - 2$ and examining the expressions of the form $a + b\alpha$, which are added and multiplied in the usual way, except that α^2 should always be replaced by 2.

Example 3. If we multiply two expressions α and $(4+\alpha)$, then we get $\alpha(4+\alpha) = 4\alpha + \alpha^2 = 4\alpha + 2$.

And in case of $\mathbb{Q}^(\sqrt[3]{2})$ we work with the expressions of the form $a + b\alpha + c\alpha^2$, and similarly while multiplying we replace α^3 by 2. We can take the same general approach while dealing with finite fields.

Example 4. We take the finite field $\mathbf{F}_3$ and construct its extension $\mathbf{F}_9$. Here we have $p = 3$ and $q = p^2 = 9$. For the construction of $\mathbf{F}_9$, we take any monic quadratic polynomial in $\mathbf{F}_3$ which has no roots in $\mathbf{F}_3$. A monic polynomial is a one variable polynomial in which the leading coefficient (the nonzero coefficient of highest degree) is equal to 1. The elements of $\mathbf{F}_3$ are $0, \pm 1$. So, we try all the possible choices for the coefficients and test whether the elements of $\mathbf{F}_3$ are its roots or not. We find that there are only three possible monic irreducible quadratics: $X^2 + 1, X^2 \pm X - 1$.

If we take a α to be a root of $X^2 + 1$, then the elements of $\mathbf{F}_9$ are combinations of $a + ib$, where a and b are 0 and ± 1 and i is the root which is equal to $\sqrt{-1}$. The arithmetic is done in the field $\mathbf{F}_9$ and the coefficients a and b occur in the field $\mathbf{F}_3$.

We know that for an element to be a generator of the finite field it should be equal to the order of the field. Now the element i is not a generator of $\mathbf{F}_9^*$ as its order is 4 while the $q - 1 = 8$. If we adjoin a root α of $X^2 - X - 1$, we can get all nonzero elements of $\mathbf{F}_9$, by taking successive powers of α(α^2 is replaced by $\alpha + 1$ since α satisfies the equatiion $X^2 = X + 1$):

$$\alpha^1 = \alpha$$

$$\alpha^2 = \alpha + 1$$
$$\alpha^3 = \alpha(\alpha + 1) = -\alpha + 1$$
$$\alpha^4 = \alpha^2 + 2\alpha + 1 = (\alpha + 1) + 2\alpha + 1 = -1$$
$$\alpha^5 = \alpha(\alpha^4) = \alpha(-1) = -\alpha$$
$$\alpha^6 = \alpha^2(\alpha^4) = (-1)(\alpha + 1) = -\alpha - 1$$
$$\alpha^7 = \alpha^3(\alpha^4) = (-1)(-\alpha + 1) = \alpha - 1$$
$$\alpha^8 = (\alpha^4)^2 = (-1)^2 = 1.$$

So, here the root of the polynomial $X^2 - X - 1$ generates the entire field and its order is equal to 8. The polynomial $X^2 - X - 1$ is known as *primitive*, meaning that any root of the irreducible polynomial is a generator of the group of nonzero elements of the field. There are $\phi(8) = 4$ generators of the field. Two generators of the field are α and its conjugate, i.e. the roots of the polynomial $X^2 - X - 1$ and the other two generators are the roots of the other irreducible polynomial $X^2 + X - 1$.

Of the remaining four elements, two are roots of the equation $X^2 + 1 = 0$ and are $\pm i$ of order four each. The other two are ± 1 with 1 being the multiplicative identity of the field and -1 having order 2.

3 Cryptography

Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. The message we intend to send is called *plain text* and the secret code is called *cipher text.* The plain text and cipher text is written in some alphabet consisting of a certain number of symbols like numerals, alphabets, blanks, punctuation marks and other usual writing symbols. *Encryption* is the process of converting a plain text into cipher text and the reverse process is known as *decryption.* The reference we follow is the text by Neal Koblitz ([1]).

To start off the *enciphering* process, we first break the plain text into message units. A message unit may be a single letter, a pair of letters (*diagraph* or a block of 50 letters. An *enciphering transformation* may be defined as a map f from the set P, the set of all possible plain texts to the set C of all possible cipher text message units. The map f has a 1-to-1 correspondence. Otherwise two plain texts having the same cipher text or some cipher text having no pre-image, i.e. no corresponding plain text will cause confusion and incorrect messages will be transmitted. The *deciphering transformation* is the f^{-1} map which recovers the original text. This situation can be explained with the help of the following diagram

$$P \xrightarrow{f} C \xrightarrow{f^{-1}} P.$$

3.1 Some simple cryptosystems

Caesar cipher. Caesar cipher is possibly the simplest and the most commonly used encryption method. Also known as *shift cipher*, in this technique each letter in the plain text is replaced by a letter some fixed number of positions ahead of its original position. For example, with a left shift of 3, E would be replaced by B, M would become J, and so on. The method is named after Julius Caesar, who first used it.

The Caesar cipher can be easily broken even in a cipher text-only scenario. Two situations can be considered:

1. An attacker knows (or guesses) that some sort of simple substitution cipher has been used, but not specifically that it is a Caesar scheme;

2. An attacker knows that a Caesar cipher is in use, but does not know the shift value.

Frequency analysis of alphabets in the plain text and cipher text is done and we match the letters which have similar frequency in both the texts and the shift of position can be found easily.

Example 1. Suppose that we have a large string of alphabets and we know that 'k' has the highest frequency in that section of the cipher text. We now that 'e' is the most occurring alphabet in the English language, i.e. our plain text. There is a shift of six positions to the right of e. Let the cipher text be 'YASSKXOTZKXT'. After deciphering this text, i.e. shifting each letter six positions to the left, we get 'SUMMERINTERN'. This is a fairly basic example where we have not taken into account the numerals, blanks and special characters.

Constructing a cryptosystem. The first step in this process is labelling the elements that make up the plain text by means of mathematical objects. Usually we label the single letters from 26-letter alphabet A$-$Z as the integers $0, 1, 2, \cdots, 25$. Thus, in place of A we write 0, and in place of S we write 18 and so on. And we assign the blank space to 26. One way to look at this system of 27 elements is using the operation of addition modulo 27.

Example 2. Suppose we are using the 26-letter alphabet A$-$Z with the numerical equivalents $0 - 25$. Let the letter $P \in \{0, 1, 2, \cdots, 25\}$ stand for a plain text message unit. Now we define a function f from the set $\{0, 1, 2, \cdots, 25\}$ to itself by the rule given below

$$f(P) = \begin{cases} P + 3 & P < 23 \\ P - 23 & P \geq 23. \end{cases}$$

f simply adds 3 modulo 26: $f(P) \equiv (P + 3)\, mod\, 26$. Then, the plain text used in the previous example 'SUMMERINTERN' becomes 'VXPPHULQWHUQ'. This example illustrates Caesar cipher in a more mathematical way.

Affine map. An improvement from the shift transformation, an affine transformation is denoted by $C \equiv (aP + b)\, mod\, N$, where a and b are fixed integers (together forming the enciphering key).

Example 3. Let us take the 26-letter alphabet and we want to encipher 'RESEARCH' using the affine transformation with the enciphering key $a = 11$, $b = 10$. We get 'PCACKPGJ'.

Deciphering an affine system requires us to solve P in terms of C , obtaining $P \equiv (a'C + b)\ mod\ N$. Here a' is the inverse of a modulo N and b' equals $-a^{-1}b$. Note that this works only if $g.c.d.(a, N) = 1$. If $g.c.d.(a, N) > 1$, then it is easy to see that more than one plain text letter will give the same cipher text letter, so we cannot recover the plain text from the cipher text. But by definition, an enciphering transformation must be a 1-to-1 map. An special case of this transformation is when we put $a = 1$ and obtain the shift transformations. When $b = 0$, it is called a *linear* transformation, meaning that the map takes a sum to a sum, i.e. if C_1 is the encryption of P_1 and C_2 is the encryption of P_2, then $C_1 + C_2$ is the encryption of $P_1 + P_2$.

Example 4. We're still working on the 26-letter alphabet system. Suppose that we know the most frequently occurring letter of cipher text is 'K', and the second most frequently occurring letter is 'D'. It is reasonable to assume that these are the encryptions of 'E' and 'T', respectively, which are the most frequently used letters in the English language. Thus, we can two equations by substituting their numerical equivalents:

$$10a' + b' \equiv 4\, mod\, 26,$$

$$3a' + b' \equiv 19\, mod\, 26.$$

The shortest way to solve the above congruences is to subtract them and by eliminating b", we obtain:

$$7a' \equiv 11 \, mod \, 26, and$$

$$a' \equiv \; 7^{-1} 11 \equiv \; 9 \, mod \, 26.$$

And now by substituting a' in the first congruence we obtain b':

$$b' \equiv (4 - 10a') \equiv 18 \, mod \, 26.$$

So, the cipher text can be deciphered by means of the formula $P \equiv (9C + 18) \, mod \, 26$.

Digraph transformations. In this technique we suppose that our plain text and cipher text is made up of two-letter blocks, called *digraphs*. This means that the plain text is split up into two-letter segments. If the entire plain text has an odd number of letters, then in order to obtain a complete set of digraphs, we add an extra letter at the end; we generally choose a blank space so that there is no much confusion.

Now each digraph is assigned a unique numerical equivalent. The simplest way to do this is to take $xN + y$, where x is the numerical equivalent of the first letter of the digraph, y is the numerical equivalent of the second letter of the digraph and N is the number of letters in the alphabet. We think of a digraph as a 2-digit base-N integer. This gives a 1-to-1 correspondence between the set of all digraphs in the N-letter alphabet and the set of all nonnegative integers less than N^2.

In the next step, we decide an enciphering transformation, i.e. a rearrangement of the integers $\{0, 1, 2, \cdots, N^2 - 1\}$. The simplest enciphering system are the affine ones, where we view this set of integers as $\mathbf{Z}/N^2\mathbf{Z}$. We define the encryption of P to be the nonnegative integer less than N^2 satisfying the congruence $C \equiv (aP + b) \, mod \, N^2$. Here also a must be prime to N^2(or rather to N), in order that we have an inverse transformation for the ciphered text. It is given by $P \equiv (a'C + b') \; mod \; N^2$ where $a' \equiv a^{-1} \; mod \, N^2$ and $b' \equiv -a^{-1} b \, mod \, N^2$. After this step we can translate C into a two-letter block of cipher text by writing it in the form $C = \; x'N + y$, and then find the letters with numerical equivalents x' and y'.

Example 5. We have a cryptosystem with a 27-letter alphabet, using digraph transformations. Each digraph represents an integer between 0 and $728 = 27^2 - 1$ according to the rule that, if two letters in the digraph have numerical equivalents x and y, then the digraph have numerical equivalent $27x + y$. An extensive study of the cipher text by frequency analysis reveals that the most commonly occurring digraphs(in order) are 'ZA', 'IA' and 'IW'. And the most common digraphs in the English language are 'E '(i.e. E followed by a blank space), 'S ', and 'T '. The cryptosystem uses an affine enciphering transformation modulo $729 = N^2$. Find the deciphering key and then read the secret message 'NDXBHO'. Also find the enciphering key.

Solution. We know that the plain text are enciphered using the rule $C \equiv (aP + b) \; mod \; 729$,and that ciphered texts can be deciphered by means of the rule $P \equiv (a'C + b') \; mod \, 729$. (a, b) form the enciphering key and (a', b') form the deciphering key. We first want to find the deciphering key. After replacing the digraphs by their numerical equivalents, we have three congruences:

$$675a' + b' \equiv 134\, mod\, 729,$$

$$216a' + b' \equiv 512\, mod\, 729,$$

$$238a' + b' \equiv 721\, mod\, 729.$$

Firstly, let us try to eliminate b' by subtracting the first two congruences. We get $459a' \equiv 351\, mod\, 729$ which does not have a unique solution of $a'\, mod\, 729$ as *g.c.d(459,729)*$\neq 1$. Instead we subtract the third congruence from the first and obtain $439a' \equiv 142\, mod\, 729$. To solve this congruency, we must find the inverse of 437 *modulo* 729. By the Euclidean algorithm we had used earlier we can get the inverse as follows:

$$729 = 427 \cdot (1) + 292$$

$$437 = 292 \cdot (1) + 145$$

$$292 = 145 \cdot (2) + 2$$

$$145 = 72 \cdot (2) + 1$$

The $g.c.d.(729, 437) = 1$ and hence we can find a unique inverse for the cipher text. And then after this process

$$\begin{aligned} 1 &= 145 - 72 \cdot (2) \\ &= 145 - 72 \cdot (292 - 145 \cdot (2)) \\ &= 145 \cdot 145 - 72 \cdot 292 \\ &= 145 \cdot (435 - 292) - 72 \cdot 292 \qquad (5) \\ &= 145 \cdot 437 - 217 \cdot 292 \\ &= 145 \cdot 437 - 217 \cdot (729 - 437) \\ &\equiv 362 \cdot 437\, mod\, 729. \end{aligned}$$

Thus, $a' = 362 \cdot 142 \equiv 374 mod 729$, and then $b' \equiv 134 - 675 \cdot 374 \equiv 647 mod 729$. Now, we apply the deciphering transformation to the digraphs 'ND, 'XB' and 'HO' of our cipher text. These digraphs correspond to the integers 354, 622 and 203, respectively. We then obtain the integers 365, 724 and 24. How?

We write $365 = 13 \cdot 27 + 14$, $724 = 26 \cdot 27 + 22$ and $24 = 0 \cdot 27 + 24$. Then we put together the plain text digraphs into the message 'NO WAY'.

At last, to find the enciphering key we compute $a \equiv a'^{-1} \equiv 374^{-1} \equiv 614\, mod\, 729$. This is carried out using the Euclidean algorithm. And $b \equiv -a'^{-1}b' \equiv -614 \cdot 647 \equiv 47\, mod\, 729$.

Although affine cryptosystems with digraphs are relatively more secure than the earlier cryptosystems. Still it has its own drawbacks which make it vulnerable to attacks. Notice that the second letter of each cipher text digraph is dependent only on the second letter of the plain text digraph. This is due to the reason that second letter depends on the mod-N value of $C \equiv (aP + b)\ mod\ N^2$, which depends only on P modulo N, i.e. only on the second letter of the plain text digraph. Thus, one could obtain a lot of information (the enciphering key a and b)from a frequency analysis of the even-numbered letters of the cipher text message.

4 Public Key Cryptography

4.1 Introduction

The cryptosystems we have been dealing with till now requires the sender to have a distinct *enciphering key* K_E and the receiver to have a unique *deciphering key* K_D. There should be some communication between the sender and the receiver where they would have to decide upon the keys that need to be used. The general procedure to encipher and decipher cannot be kept secret but what we can control is the keys that will be used.

Need for a better system. Why was a new type of cryptosystem is required? Some of the decisive reasons for the need are as follows:

1. A disadvantage of private key cryptography is that the keys must be shared before they can be used. The sharing process has to be secure, since a person who intercepts the private key undetected can decipher messages that he subsequently intercepts.

2. Another disadvantage of private key encryption is that if the key becomes known by unauthorized individuals, the key is compromised and must be regenerated and redistributed.

3. Since keys are subject to potential discovery by a cryptographic adversary, they need to be changed often and kept secure during distribution and in service.

The idea of public key cryptography. A public key cryptosystem has the property that someone who knows only how to encipher the plain text cannot use the enciphering key to find the deciphering key without a extremely long computation. An extra bit of information is required that is kept private with the receiver. In totality, our aim is to find an enciphering function $f : P \longrightarrow C$ that is easy to compute once the enciphering key is known but it is very hard to compute the inverse function $f^{-1} : C \longrightarrow P$. We can say that the function f is practically not possible to invert, i.e. is not invertible. Such a function f is called a $trapdoor\ function$.

A trapdoor function f is a function which is easy to compute in one direction but whose inverse f^{-1} is hard to compute without having some extra bit of information. This information is the deciphering key K_D which makes it easy to compute the inverse f^{-1}.

Authentication. *Signature* is the most important part of a message. A person's signature written in an unique and peculiar flow of the pen is hard to duplicate. It lets the recipient know that the message really is sent from the person whose name is typed below. Important messages are required to be authenticated using additional methods to communicate. When we don't have a physical signature, we have to rely entirely on other methods. For instance, when an officer of a corporation wants to withdraw money from the corporate account by telephone or when he forgets the password to his Internet Banking account, he is asked to give personal information like his pet name or the place of his birth which only the corporate officer knows and the bank knows. But an imposter would have a hard time figuring out this particular piece of information.

In public key cryptography there is an especially easy way to identify oneself in such a way that no one could be pretending to be you. Let A(Amit) and B(Bani) be two users of the system. Let f_A be the enciphering transformation with which any user of the system sends a message to Amit, and let f_B be the same for Bob. For a easier example, we suppose that the set P of all possible plain text message units and the set C of all possible cipher text message units are equal, and are the same for all the users. Let S_A be Amit's signature (which could be a identification number or the time of the communication, etc.) It would not be enough for Amit to send Bob the encoded message $f_B(S_A)$, since everyone knows how to do that and so there would be no way of knowing that the signature was not fake. Rather, for verification at the beginning of the message Amit transmits $f_B {f_A}^{-1}(S_A)$. Then, when Bani deciphers the whole message along with the ciphered signature, by applying ${f_B}^{-1}$, he finds that everything has become plain text except for a small section of unreadable text, which is ${f_A}^{-1}$. Now since Bani knows that the message is claimed to be from Amit, she applies f_A(which she knows since Amit's enciphering key is public), and obtains S_A. Since no other than Amit could have applied the trapdoor function ${f_B}^{-1}$ which is inverted by f_A, she knows that the message is from Amit.

Hash functions. A common way to sign a document digitally is with the help of a *hash* function. Plainly speaking, a hash function is a easily computable map $f \ : \ x \to h$ from avery long input x to a much shorter output h. For instance, from strings of about 10^6 bits to string of 100 or 200 units. The hash function has the property: *it is not computationally feasible to find two different inputs x and x' such that $f(x) = f(x')$.* If part of Amit's "signature" consists of the hash value $h = f(x)$, where x is the entire text of her messag, then Bani can verify not only that the message was really sent by Amit, but also that it wasn't tampered with during transmission. Bani applies the hash function f to his deciphered plain text from Amit, and cross checks whether the result matches with the value h in Amit's signature. By assumption, no tamperer would have been able to change x without changing the value of $h = f(x)$.

Key exchange. In practical use, even though the public key cryptosystems are safer than the classical systems but sending messages tend to be slower to implement in comparison to the classical systems. The number of plain text message units transmitted per second is comparatively less. However, even if a network of users feel attached to the traditional type of cryptosystem, they want to use make a auxiliary use of the public key cryptosystem to send each other their personal keys $K = (K_E, K_D)$ for the classical system. Therefore the ground rules for the classical cryptosystem are agreed upon wherein the large volume of messages would be sent by the faster, older methods and the keys can be periodically exchanged using the slower public key cryptography.

Probabilistic Encryption. The encryption methods we have used till now have been *deterministic* or rather most of the number theory based cryptosystems for message transmission are *deterministic*. It means that a given plain text will always have the same cipher text at any given time it is sent.

However, deterministic encryption has two disadvantages:

1. If an eavesdropper knows that the plain text message belongs to a small text(for example, the message is either ”yes” or ”no”), then she can simply encrypt all possibilities in order to determine which is the secret message.

2. It seems to be very difficult to prove anything about the security of a system if the encryption is deterministic.

For the above reasons, *probabilistic encryption* was introduced. We will not be discussing much about this type of encryption.

4.2 RSA

On our way to finding a function whose decryption is infeasible, we end up looking at an ancient problem of number theory: the problem of finding the complete factorization of a large composite integer whose prime factors are not known. The RSA cryptosystem, named after Rivest, Shamir and Adleman who established it, is the oldest and the most popular public key cryptosystems, is based on the tremendous difficulty of factoring a large number.

We now learn how to connect the phi-function to modular exponentiation. For this we turn to Euler’s theorem which is a relationship between the phi-function and modular exponentiation as follows:

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

This means we could pick any two numbers such that do not share a common factor, let’s call them m and n, say $m = 5$ and $n = 8$. Now when raise m to the power of $\phi(n)$ and divide by n, we always get 1 as the remainder.

$$5^4 \equiv 625 \equiv 1 \, mod \, 8.$$

Now we just need to modify this equation using two simple rules.

1. If we raise the number 1 to any exponent k, we always get 1, i.e. $1^k = 1$. And in the same way we can multiply the exponent $\phi(n)$ by any number k and the solution is still 1.
$$m^{k*\phi(n)} \equiv 1 \, mod \, n$$

2. If we multiply 1 by any number, say m the number is still m, i.e. $1 * m = m$. Similarly we can multiply the left side of the previous congruence by m to get m on the right hand side.
$$m^{k*\phi(n)+1} \equiv m \, mod \, n$$
This is the breakthrough. We now have a equation for finding e times d which depends on $\phi(n)$.
$$m^{e*d} \equiv m \, mod \, n$$

Therefore it is easy to calculate d only if the factorization of n is known. It means that d should Amit's private key. It is the trapdoor which will allow her to undo the effect of e. Lets go through a simple example to see all this in action.

Example 1. Say Bani has a message she converted into a number using a padding scheme. Let's call this n. Then Amit generates her public and private key as follows. First he generates two random prime numbers of similar size , let $p_1 = 53$ and $p_2 = 59$ and multiply them to get $n = p_1 * p_2 = 53 * 59 = 3127$. Then he calculates $\phi(n) = \phi(3127) = 52 * 58$ easily because he knows the factorization of n. Next he picks some small public exponent e with the condition that it must be an odd number that does not share a factor with $\phi(n)$. Let $e = 3$. Finally he finds the value of his private exponent d which is
$$d = 2 * (\phi(n) + 1)/3 \, or \, d = 2011$$
. Now he hides everything except the value of n and e which make up the public key. Think of it as a open lock. He sends this to Bani to lock his message with. Bani locks his message by calculating m to the power of $e \, mod \, n$. Let $m = 89$.
$$89^3 \, mod \, 3127 \equiv 1394.$$
Call this $C = 1394$, the encrypted message which she sends back to Amit. Finally Amit decrypts using his private d accessed through his trapdoor. c to the power $d \, mod \, n$ equals Bani's original message m.
$$1394^2 011 \equiv 89 \, mod \, 3127.$$
Notice that Eram, the eavesdropper with C, n and e can only find the exponent d if they can find $\phi(n)$ which requires that she knows the prime factorization of n which is not possible to compute.

RSA Encryption Algorithm. We now describe the RSA algorithm. Each user first chooses two very large prime numbers p and q, and sets $n = pq$. Knowing the factorization of n, it is easy to compute $\phi(n) = (p-1)(q-1) = n+1-p-q$. Next we randomly choose an integer e between 1 and $\phi(n)$ which is prime to $\phi(n)$. The "random" number chosen is generated by a computer program that generates a sequence of digits in a way that no one could duplicate or predict and this randomness helps. On the other side, if we choose the same number or choose from a small collection of digits, then the system becomes incredibly unsafe. The random number e is prime to $\phi(n)$ and should be chosen randomly between numbers 1 and $\phi(n)$.

So firstly each user chooses two primes p_A and q_A and a random number e_A which has no common factor with $\phi(p_A q_A) = (p_A - 1)(q_A - 1)$. Next we compute $n_A = p_A q_A$ and multiplicative inverse of e_A modulo $\phi(n_A)$: $d_A = {e_A}^{-1} \, mod \, \phi(n_A)$.

After this Amit makes public the enciphering key $K_{E,A} = (n_A, e_A)$ but conceals the deciphering $K_{D,A} = (n_A, d_A)$. The enciphering transformation is a map from $\mathbf{Z}/n_A\mathbf{Z}$ to itself given by the function $f(P) \equiv P^{e_A} \, mod \, n_A$. Similarly the deciphering transformation is the map from $\mathbf{Z}/n_A\mathbf{Z}$ to itself given by the function $f^{-1}(C) \equiv C^{d_A} \, modn_A$. It is easy to observe that the two maps are inverse of each other, because of our definition of d_A. Performing the function f followed by f^{-1} or f^{-1} followed by f means raising to the $e_A d_A$-th power. But, because $e_A d_A$ leaves a remainder of 1 when divided by $\phi(n_A)$, this is the same thing as raising to the 1-st power. We better understand the working of the system from the following example.

Example 2. We propose a system where plain text consists of trigraphs and the cipher text consists of four-graphs in the usual 26-letter alphabet. To send the message "YES" to Amit with the enciphering key $(n_A, e_A) = (46927, 39423)$, we first find the numerical equivalent of "YES" as follows:

$$24 \cdot 26^2 + 4 \cdot 26 + 18 = 16346,$$

and then compute $16346^{39423} \, mod \, 46927$, which is

$$21166 = 1 \cdot 26^3 + 5 \cdot 26^2 + 8 \cdot 26 + 2,$$

and this is equivalent to "BFIC". The recipient Amit knows the deciphering key $(n_A, d_A) = (46927, 26767)$, and so computes

$$21166^{26767} \, mod \, 46927 = 16346,$$

which in turn is equal to "YES". Another question that might arise is that how did Amit generate his keys? First, he multiplied the primes $p_A = 281$ and $q_A = 167$ to get n_A; then he chose e_A at random, subject to the condition that $g.c.d.(e_A, 280) = g.c.d.(e_A, 166) = 1$. Then he found $d_A = e_A^{-1} \, mod \, (280 \cdot 160)$. And the numbers p_A, q_A and d_A remain secret.

5 Concluding Remarks

In the last example we may think that the computations will get quite cumbersome when we take very large primes. But this is not in the case. The most time consuming step is modular exponentiation. But this could be achieved by the repeated squaring method. Potentially the most time consuming step is finding the two large prime numbers without knowing the factorization of the actual number. We don't have to worry about this because this process is not needed in secure communication. On the other hand this step makes the cryptographic system practically unbreakable.

We discussed only one type of trapdoor function here. Several important algorithms in public-key cryptography base their security on the assumption that the discrete logarithm problem over carefully chosen groups has no efficient solution. There exist groups for which computing discrete logarithms is apparently difficult. In some cases (e.g. large prime order subgroups of groups Z_p^*) there is no efficient algorithm known for the worst case. At the same time, the inverse problem of discrete exponentiation is not difficult (it can be computed efficiently using exponentiation by squaring).

Another type of public key cryptography is making the use of Elliptic curves. In mathematics, an elliptic curve is a plane algebraic curve defined by an equation of the form $y^2 = x^3 + ax + b$ that is non-singular, i.e. it's graph has no cusps or self intersections. Elliptic curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. ECC requires smaller keys compared to non-ECC cryptography (based on plain Galois fields) to provide equivalent security. The primary advantage of using Elliptic Curve based cryptography is the reduced key size and hence faster speed. Elliptic curve based algorithms use significantly smaller key sizes than their non elliptic curve equivalents. The difference in equivalent key sizes increases dramatically as the key sizes increase.

Public-key cryptography is used to secure electronic communication over an open networked environment such as the Internet, without relying on a hidden channel, even for key exchange. Combining public-key cryptography with an Enveloped Public Key Encryption method, allows for the secure sending of a communication over an open networked environment. And nowadays no communication can happen without the guarantee of an secure connection. It is practically impossible to work safely in the present world without using cryptography systems.

6 Bibliography

1. Neal Koblitz, A Course in Number Theory and Cryptography, Second Edition, Springer-Verlag New York, 1994.

2. Patrick Morandi, Field and Galois Theory, First Edition, Springer-Verlag New York, 1996.

3. David M. Burton, Elementary Number Theory, Fifth Edition, McGraw Hill Education, 2002.