CRYPTOGRAPHY AND FACTORIZATION METHODS IN CRYPTOGRAPHY

By

SUBRAMANYAM DURBHA

A thesis submitted to the

Graduate School-Camden

Rutgers, the State University of New Jersey

In partial fulfillment of the requirements

For the degree of Master of Science

Graduate Program in Mathematics

Written under the direction of

Prof. Will Y.K. Lee

And approved by

_____

Prof. Will Y.K. Lee

Camden, New Jersey

January 2018

THESIS ABSTRACT

Cryptography and Factorization Methods in Cryptography

by SUBRAMANYAM DURBHA

Thesis Director:
Prof Will Y.K. Lee

The Security of the RSA cryptosystem depends on the difficulty of the prime factors of large integers. Here we explore some of the factorization techniques currently available in cryptography. After giving an overview of cryptography we discuss some of the factorization techniques like Fermat's factoring, Pollards p-1 method and continued fraction method. We then explore the theory of binary quadratic forms and its applications to factorization.

Table of Contents

Part I - An overview of Mathematical Cryptography p 1-13

Part II - Factorization techniques - Fermat's factoring, pollards p-1 method, continued fraction method. p 13 - 21

Cryptography, is the Methodology of concealing the contents of messages. The Modern scientific study of cryptography is sometimes referred to as Cryptology. Plaintext is the original message in readable form. Cipher text is the encrypted message. For example the following plaintext Enemy falling back- Breakthrough imminent Lucius is encrypted as follows

EnemyfallingbackbreakthroughimminentLucius - Plaintext

Jsjrdkfqqwslgfhpgwifpymwtzlmnrrnsjsyqzhnzx - Ciphertext

By using a Caeser cipher where each letter is shifted 5 letters up in the alphabet. When you are at the end of the alphabet you wrap around

for example y → z a b c d y is encrypted as d.

A simple substitution Cipher is any permutation of the alphabet. A Caesar Cipher is a particular form of simple substitution Cipher. There are 26! simple substitution Ciphers.

The following is the scenario in which we discuss problems in Cryptography. Alice wants to send a secret message to Bob. Eve is trying to intercept the message and read the messages

Alice ----------→ Bob

↑

Eve (Evesdropper)

If Alice wants to send a message to Bob using a simple substitution cipher and Eve intercepts one of the messages and does not know the key. To make an exhaustive search she has to check 26! ~ 10^{26} possibilities and using the fastest computer available it will take her more than 10^{13} years which is more than the estimated age of the universe. An exhaustive search is infeasible.

Although the number of possible substitution ciphers are quite large decrypting a cipher text built on a simple substitution cipher is not that difficult, if she makes a statistical analysis of the frequency of the various letters in the Cipher text .For example if the letter C is the most occurring letter in the cipher text followed by S according to the statistical distribution of letters in Common English text C should correspond to E and S should correspond to t etc., and she can recover the plaintext after some effort.

Mathematical Preliminaries

N denotes the set of natural numbers { 1,2,3,4,5,6,7,8,9, ….}

Z denotes the set of integers { -5,-4,-3,-2,-1,0,1,2,3 }

a divides b (a | b)

If ∃ $k \in Z$ such that b = ak

example 3|12, 6|18, 7|14

Facts If a | b b | c a | c

a | b b | a ⇒ a = ± b

a | b a | c Then a | b ± c

The Greatest Common divisor of the integers a and b denoted (a, b) is the largest among all the common divisors of a and b

e.g., (12, 18) = 6

(748, 2024) = 44

The division Algorithm:

Let a, b be positive integers ∃ integer q and r such that

a= bq + r $0 \leq r < b$ [The usual quotient and remainder]

The Euclidean Algorithm for finding the G.C.D of a and b

Apply division algorithm

$a = bq_1 + r_1 \qquad 0 \le r_1 < b$

$b = r_1q_2 + r_2 \qquad 0 \le r_2 < r_1$

$r_1 = r_2q_3 + r_3 \qquad 0 \le r_3 < r_2$

.

.

.

$r_{k-2} = r_{k-1}\, q_k + r_k \qquad 0 \le r_k < r_{k-1}$

$r_{k-1} = r_k \quad q_{K+1}$

The last non zero remainder rk is the g.c.d (a,b)

Reason: $b > r_1 > r_2$ …….

The sequence decreases and finally you should reach 0.

The last non zero remainder r_K is the G.C.D of a and b

$(a,b) = (b, r_1) = (r_1, r_2). = (r_{k-1}, rk) = r_k$

The number of steps is at most $2 \log_2 b + 1$

Example

(2024, 748) = 44

2024 = 748(2) + 528

748 = 528(1) + 220

528 = 220(2) + 88

220 = 88(2) + 44 → GCD

88 = 44(2)

From last equation 44 = 220 – 88(2). Working backward replacing for 88 we find

2044 can be expressed as

2024(-7) + 740 (19) = 44

In general (a,b) = ax + by.

For some integers x and y.

If (a,b) = 1 (i.e. a, b relatively prime)

Then ∃ integers x and y such that ax+ by = 1

Modular Arithmetic

We say a Ξ b (mod m) a, b, m integers

If m | a – b

e.g 10 Ξ 2 (mod 4) since 4 | 10 -2 = 8

15 Ξ 3(mod 6) since 6 | 15 – 3 = 12

Some Facts (Results)

If a Ξ b (mod m)

c Ξ d (mod m) then

1) a ± c Ξ b ± d (mod m)

ac Ξ bd (mod m)

2) If (a, m) = 1 ∃ an integer b such that ab Ξ 1 (mod m)

In fact, a, 2a, 3a ……..... (m – 1) a leave the remainders 1, 2 …. (m -1) in

Some order. Therefore, ∃ b such that ab Ξ 1 (mod m) b is called inverse

of a

i.e., $b = a^{-1} \pmod m$

Example: (2, 5) = 1

b = 3 is the solution to 2b Ξ 1 (mod 5)

$3 = 2^{-1} \pmod 5$

(4, 15) = 1 $4 = 4^{-1} \pmod{15}$
Since 4 (4) Ξ 1 (mod 15)

We write Z/ m Z = {0, 1, 2, 3…… (m -1) }

Remainders on division by m

F_p = {0, 1, 2, 3 ….. p-1}

F p* = {1, 2, 3 ……. p -1}

(Z/mZ) * = {a ∈ Z/mZ | (a, m) =1}

= {a ∈ Z/mZ | a has inverse mod m}

(Z/mZ) * is called the group of units mod m

e.g., (Z /24 Z) * = {1, 5, 7, 11, 13, 17, 19, 23}

(Z/ 7 Z) * = {1, 2, 3, 4, 5, 6}

Φ (m) = # {a : 0 ≤ a < m (a, m) = 1}

Φ (24) = 8

For a prime p, Φ(p) = p – 1. If the letters of the alphabet are assigned the values 0, 1, 2, 3…. 25

A Shift cipher (or Caesar Cipher) is described by

encryption c Ξ p+ k mod 26

Decryption p Ξ c - k mod 26 for a fixed k ≥ 0

Often in Cryptography we are required to compute g^A mod N for a large value of N (consisting of hundreds of digits) where g is a non-zero integer and A is large exponent.

A naïve way is to compute

g Ξ g_1 mod N

g_2 Ξ g^2 Ξ g g_1 mod N

$g_3 \equiv g^3 \equiv g\, g_2 \mod N$

Infeasible if A is very large we have a faster algorithm called the fast

powering algorithm to do this more efficiently. We write A in base 2 (i.e.,

as sum of powers of 2)

e.g we want to compute $3^{218} \mod 1000$

we have $218 = 2 + 2^3 + 2^4 + 2^6 + 2^7$

$3^{218} = 3^2 \times {}_3 2^3 \times {}_3 2^4 \times {}_3 2^6 \times {}_3 2^7$

It is relatively easy to compute 3, ${}_3 2$, ${}_3 2^2$, ${}_3 2^3$, ${}_3 2^4$ ….

Since each is the square of the preceding we form the table

i	0	1	2	3	4	5	6	7
${}_3 2^1$ Mod 1000	3	9	81	561	721	841	281	961

$3^{218} \equiv 9.561.721.281.961 \mod 1000$

$\equiv 489 \pmod{1000}$

Much faster than the naïve approach (Totally 11 multiplications)

Fundamental Theorem of Arithmetic

Any integer $a \geq 2$ can be written $a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$

$p_1 p_2 .. p_k$ distinct primes $\alpha i \in N \quad i = 1,2,3 .. k$

Called the prime factor decomposition. The decomposition is unique up to the order of

the primes.

Let $a \in Z/ pZ = \{0, 1, 2\ldots. (p-1)\}$

p prime $a \neq 0 \ \exists\ b \neq 0 \in Z/ pZ$

Such that $ab \equiv 1 \pmod p$ Since $(a, p) = 1$

To compute a^{-1} we simply find u, v such that

a U + P V = 1 (by the EA)

Then a U $\equiv$ 1 mod p

$a^{-1} = U \bmod p$

computing inverses in (Z/pZ) * = Fp * is easy

Primitive Roots

Fermat's Little Theorem

Let p be a prime and (a,p) = 1 then $a^{p-1} \equiv 1 \bmod p$

e.g (3, 5) = 1 5 prime

$3^{5-1} = 3^4 \equiv 1 \pmod 5$ since 81 – 1 = 80 $\equiv$ 0 mod 5)

e.g. p = 15485863 is prime $2^{15485862} \equiv 1 \pmod{15485863}$ without any computation we know this.

By Fermat's Theorem if g $\in$ {1, 2 (p -1)} $g^{p-1} \equiv 1 \pmod p$

If p-1 is the lowest such power (i.e., $g^x \not\equiv 1 \pmod p$ for $0 < x < p-1$)

g is called a primitive root mod p. In this case $\{1, g, g^2 \ldots g^{p-2}\} = F_P^*$

Result

If p is a prime of $\exists$ a primitive root mod p, In fact p has Φ (p-1) primitive roots.

(Φ is Euler's totient function)

Symmetric Ciphers

A Cipher in which Bob and Alice have equal knowledge and capabilities.

Encoding Schemes

It is convenient to view plaintexts, keys and cipher texts as numbers and to write those numbers in binary form Using the ASCII (American Standard Code for Information exchange)

The Phrase "Bed bug" is encoded as

B	e	d	spacing	b	u	g	.
66	101	100	32	98	117	103	46

01000010 01100101 01100100 001000000 01100010 0110101 01100111 001011

Where each number is converted into a string of 8 bits. In this way the whole plaintext is converted into a sequence of 0's and 1's. We divide the plaintext into blocks of bits of size B and do encryption one block at a time. In this way need to concentrate only on bits of block size B.

$m_{b-1}\ m_{b-2} \ldots m_0$ —> converted to the corresponding number in binary form

$$m_{b-1}\, 2^B + m_{b-2}\, 2^{B-2} + m_o < 2^B$$

in this way we have M the set of all plaintext messages

$M = \{m: 0 \le m < 2^{B_m}\}$

$K = \{k: 0 \le k < 2^{B_K}\}$

$C = \{c: 0 \le c < 2^{B_C}\}$

K is the set of all keys C is the set of all cipher texts

Encryption and decryption is done one block at a time. B_k, B_m, B_c need not be equal.

Let P be a prime (large). How large should the key size be so that Bob and Alice can safely exchange messages without worrying about Eve intercepting and decrypting them?

If Bk is chosen such that Bk ≥ 80 an exhaustive search for the key is considered infeasible. In some cases where meet in the middle collision attacks are available Bk should be chosen ≥ 160.

Example

Let $2^{159} < p < 2^{160}$ where p is a prime.

Let K = M = C = {1, 2 … (p -1)} = Fp *

Alice and Bob select a key k, 1 ≤ k < p

The encryption is done by the function

$$e_k (m) = c \equiv k\ m \bmod p$$

decryption by

$$d_k (c) = k^{1}c \bmod p$$

k^1 is inverse of k mod p

$$d_k (c) = k^{1}c \equiv k^{1}km \equiv m \bmod p$$

Computing k^1 from k is easy if we know k.

Eve has a hard time guessing k because of the size of the key space K. Even if she intercepts a message and obtains a cipher text it is still difficult to get hold of K.

Symmetric Ciphers assume Bob and Alice meet beforehand to agree on a secret key K. What if they don't have this opportunity and every communication between them monitored by Eve? This is possible by the Daffie Hellmann key exchange which relies on the difficulty of solving the discrete logarithm problem which is to solve

$$g^{x} \equiv h \bmod p$$

for x given g, h and p. p a large prime and g a primitive root mod p.

Asymmetric Ciphers

As usual we have

K = {the space of Keys}

M = the space of plaintext messages

C = the space of Cipher text messages

A Key K = (K priv, K pub)

↓ ↓

Private Key Public key

for each K_{pub} there is an encryption function e_{kpub} : M —> C

and for each kpriv there is a decryption function d_{kpriv} : C —> M

such that dk_{priv} (e_{kpub} (m)) = m for every m ∈ M

Note that Alice can send Bob kpub over an insecure communication channel without worrying about Eve decrypting it because it is difficult for Eve to decrypt without knowing the function d_{kpriv} even if she knows k_{pub}.

The RSA System

Some Preliminary results. let p, q be distinct primes

Let g = (p -1, q -1)

Then $a^{(p-1)(q-1)/g} \equiv 1 \pmod{pq}$

For every a such that (a, pq) =1

In particular $a^{(p-1, q-1)} \equiv 1 \pmod{pq}$ if (a,pq) = 1

The Diffie-Hellman Key exchange and El-Gamal PKC rely on the difficulty of solving

$a^x = b \bmod P$

a, b, p know p a large prime X unknown.

The RSA relies on the difficulty of solving $x^e \equiv C \pmod{N}$

N, C, e are known quantities X unknown. i.e., it relies on the difficulty of taking e^{th} roots mod N. If N is a prime then taking eth roots is comparatively easy by the following proposition.

Propositions: Let p be a prime and let e ≥ 1 be an integer such that (e, p -1) = 1

∴ ∃ d such that de Ξ 1 (mod p -1) then X^e Ξ c (mod p) has unique solution

X Ξ c^d (mod p)

Since it is easy to compute d it is easy to solve the above congruence.

If N = pq a product of 2 primes then it is again easy to solve the congruence.

If we know p and q but difficult if we do not know the factorization of N = pq

By a similar proposition as above we have proposition. Let p, q be distinct primes

Let e ≥ 1 and N = pq and (e, (p-1) (q-1)) = 1

Let d be an integer such that de = 1(mod (p-1) (q-1)) then $x^e \equiv c \pmod N$ has the unique solution $X \equiv c^d \bmod N$

Example:

Solve: $X^{17389} \equiv 43927 \pmod{64349}$

↓ ↓

C N

N = 64349 = 229.281 product of 2 primes. First step solve

17839 d Ξ 1 (mod 228.280)

i.e 17839 d Ξ 1 (mod 63840)

Solution is d = 53509(mod 63840) $x \equiv c^d \equiv 43927^{53509} \equiv 14458 \pmod{64349}$

Is the solution to $X^{17389} \equiv 43927 \pmod{64349}$

Alice Challenges to solve $X^{9843} \equiv 134872 \pmod{(30069476293)}$

e = 9843 c =134872 N = 30069496293

N is not a prime since $2^{N-1} \equiv 18152503636 \not\equiv 1 \bmod N$

It happens N is a product of 2 primes. If Eve does not know the factors she has hard time solving the congruence. She accepts defeat. Alice informs Eve

30069476293 = 104729.287117

With this new knowledge Alice's challenges becomes easy

Eve Solve 9483 d Ξ 1 (mod 104728.287116)

i.e computes d Ξ18472798299 (mod 30069084448) and computes the solution

X Ξ $134872^{18472798299}$ Ξ 2547028026 (mod 30069476293)

RSA Public Key System

BOB	ALICE
Bob chooses secret primes p,q chooses encryption key e such that (e, (p-1) (q-1)) = 1 publishes N, e	
	Alice chooses plaintext m uses Bobs public key (N,e) to compute C Ξ m^e mod N sends cipher text C to Bob
Bob solves the congruence de Ξ 1 (mod (p-1) (q-1)) computes m^1 Ξ c d mod N then m^1 = the plain text m	

Example - **RSA Key Creation**

Bob chooses two secret primes p =1223 q = 1987

Bob computes the public modulus N = pq = 2430101

Bob chooses a public encryption exponent e = 948047 such) that

(e, (p-1) (q-1)) = (948047, 2426892) = 1

RSA Encryption

Alice converts her plain text into an integer m = 1070777 1 ≤ m < N

Alice computes C Ξ m^e Ξ 1070777^{948047} (mod 2430101)

C Ξ 1473513 (mod 2430101) Alice sends C to Bob.

RSA decryption

Bob knows (p-1) (q-1) = 1222.1986 =2426892

He solves de Ξ 1 (mod (p-1) (q-1)) i.e., 948047d Ξ 1 (mod 2426892) and finds

d = 1051235. Then bob computes $c^d \bmod N$

i.e. $1473513^{1051235} \equiv 1070777 \pmod{243010}$

The value he computes is Alice's message m = 1070777.

In the above example the modulus n is small and Eve will not take much time to factor

in a computer. However, if p,q are chosen large Eve will have a tough time finding m because of her difficulty of factoring N when N has hundreds of digits.

Having understood the importance of factorization in the RSA Cryptosystem. We now concentrate on the factorization techniques currently. We concentrate on only 3 techniques 1) Fermat factoring 2) Pollards p -1method and 3)the continued fraction method.

Fermat Factoring

First we define the integer factoring problem (IFP) Given an integer $n \in N$ to find primes

p_i I = 1, 2 … k such that $n= P1^{\alpha 1}\ P2^{\alpha 2}\ \ldots.\ Pk^{\alpha k}$ P1< p2 < …. Pk

$\alpha_i \in N$ 1 2 4… K

A simpler problem is the problem of splitting which is to find two factors r,s of n such that n = rs $1 < r \leq s$ Since RSA modulus is a product of 2 primes both IFP and splitting are same in the case of RSA

Fermat Factoring

Suppose n = rs n, odd and r< s

Then $r \leq \sqrt{n}$ now $n = rs = (r+ s /2)^2 – (r – s/2)^2 = a^2 – b^2$

$a^2 – n= b^2$ $a = r + s /2 > \sqrt{n}$

This is true if $r + s > 2\sqrt{n}$

If $r^2 + 2rs + s^2 \geq 4n$ If $r^2 + s^2 > 2n = 2rs$ which is true

This suggest that we try

$X^2 - n$ $X = [\sqrt{n}] + 1, [\sqrt{n}] + 2 \ldots\ldots n - 1/2$ till we get a square

i.e. Suppose $a^2 - n = b^2$ then $n = a^2 - b^2 = (a + b)(a - b)$ and we have factored n

We are essentially looking for solutions of $x^2 \equiv y^2 \bmod n$, If $x \neq \pm y \pmod{n}$, $(x \pm y, n)$ will give non trivial factors of n. The running time can be shown to be a $0(n^{1/2})$

Example

We factor N = 25217 by looking for an integer b making $N + b^2$ a proper square.

$25217 + 1^2 = 25218$

$25217 + 2^2 = 25221$

$25217 + 3^2 = 25226$

$25217 + 4^2 = 25233$

$25217 + 5^2 = 25242$

$25217 + 6^2 = 25253$

$25217 + 7^2 = 25266$

$25217 + 8^2 = 25281 = 159^2$

$25217 = 159^2 - 8^2 = 167.151$

Sometimes $N + b^2$ does not become a square for a succession of Values.

If N is large it is unlikely that a randomly chosen b will make $N + b^2$ a perfect square. Then instead of N we look at a multiple of N, kN.

If $kN = a^2 - b^2 = (a + b)(a - b)$

There is a good chance N will have a nontrivial factor with each of $a + b$ or $a - b$ then it is easy to find the factor by finding $(a \pm b, N)$

Example

N = 2032999

$N + b^2$ is not a square for b = 1, 2 … 100 we now look at 3 $N + b^2$ ($2N + b^2$ cannot be a square)

$3.203299 + 1^2 = 609898$ not a square

$3.203299 + 2^2 = 609901$ not a square

$3.203299 + 3^2 = 609906$ not a square

$3.203299 + 4^2 = 609913$ not a square

$3.203299 + 5^2 = 609922$ not a square

$3.203299 + 6^2 = 609933$ not a square

$3.203299 + 7^2 = 609946$ not a square

$3.203299 + 8^2 = 609961 = 781^2$

$3.203299 = 781^2 - 8^2 = 789.773$

We compute (203299, 789) = 263 (203299, 773) = 773

We find 203299 = 263 × 773 263, 773 are primes and this is the full factorization of N

Pollards p -1 Method

Pollards p-1 method demonstrates that there are insecure RSA moduli which at first glance appear secure. We are presented with N = pq and want to find p,q. Suppose by luck or hard work or some other method we find an integer L. Such that p-1 | L but q – 1 does not divide L

Then L = i (p-1)

L = K (q -1) +j 0 < j < q -1

For a randomly chosen a, $a^L = a^{i(p-1)} \equiv 1 \bmod p$ (Fermat's title theorem)

$a^L \equiv a^j \bmod q$ since $j \neq 0$ It is unlikely $a^j \equiv 1 \bmod q$ therefore $P \mid a^L - 1$ q does not divide by $a^L - 1$ with high probability. But this is good for we can recover p by computing $(a^L - 1, N)$ [Note we use q does not divide $a^L - 1$] For otherwise $(a^L - 1, N) = N$ How can we find such L ? If p -1 has small prime factors then p-1|n! for not too large values of N.So here is the idea for each n = 2,3 .. compute $(a^{n1}-1, N)$

We take a = 2 in practice IF G.C.D=1 we go to next step If somewhere GCD = N we are unlucky. May be some other a will work. Otherwise we have a nontrivial factor of N. $a^{n1} - 1$ is quite large e.g $2^{100!} - 1$ is a number greater than the number of elementary particles in the universe. Luckily we don't need $2^{100!} - 1 (\bmod N)$ all we need is $2^{100!} - 1 \bmod N$. So we don't need to work with numbers > N. Secondly we do need to compute n!

Assume we computed $a^{n!} \bmod N$ $a^{(n+1)!} \bmod N = (a^{n!})^{n+1} \bmod N$ so we have to raise to the power n + 1 the previous step an d the fast powering algorithm does it easily $a^{n!} \bmod N$ can be computed in $2n \log_2 n$ steps. It is possible to compute $a^{n!} \bmod N$ for reasonably large values of n. We use pollards p-1 method to factor N = 13927189 starting with $(2^{9!} - 1, N)$

$2^{9!} - 1 \equiv 13867883 \pmod{13927189}$ $(2^{9!} - 1, 13927189) = 1$

$2^{10!} - 1 \equiv 5129508 \pmod N$ $(2^{10!}-1,N) = (5129508, N) = 1$

$2^{11!} - 1 \equiv 4905233 \pmod N$ $(2^{11!}-1,N) = 1$

$2^{12!} - 1 \equiv 6680550 \pmod N$ $(2^{12!}-1,N) = 1$

$2^{13!} - 1 \equiv 6161077 \pmod N$ $(2^{13!}-1,N) = 1$

$2^{14!} - 1 \equiv 879290 \pmod N$ $(2^{14!}-1,13927189) = (879290, 13927189) = 3823$

We have a non-trivial factor of N =13927189 3823 is a prime Since the other factor of 13927189 / 3823 = 3643 which also prime 13927189 = 3823 * 3643

The Continued Fraction Method

Finite Continued Fractions

An expression of the form $\alpha = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{\ddots + \cfrac{1}{q_k}}}}$

where $q_i \in R \quad q_i > 0$ for $i > 0 \quad k \in Z$

k a non- negative integer is called a continued fraction.

This is also written as $q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_K}}}$

or $(q_0 ; q_1, q_2 \ldots\ldots\ldots\ldots\ldots\ldots q_K)$

Example $\frac{10001}{210} = (4; 1, 3, 3, 2)$

If $q_i \in Z$ then the continued fraction is called a finite simple continued fraction.

Every rational number can be expressed as a finite simple continued fraction.

Convergents

Let $\alpha = (q_0 ; q_1, q_2 \ldots q_L)$ $L \in N$ be a finite continued fraction.

Let $c_k = (q_0 ; q_1, q_2 \ldots q_k)$ $k \leq L \quad k \in Z$ C_k is called the k^{th} convergent of α

$C_k = A_k / B_k$ where A_k and B_K are given by

$A_{-2} = 0 \quad A_{-1} = 1 \quad A_k = q_k A_{k-1} + A_{k-2}$

$B_{-2} = 0 \quad B_{-1} = 1 \quad B_k = q_k B_{k-1} + B_{k-2}$

$Ck = \frac{A_k}{B_k} = \frac{q_k A_{k-1} + A_{k-2}}{q_k B_{k-1} + B_{k-2}}$

If C_k is the k^{th} convergent $c_1 > c_3 > c_5 > C_{2k-1} > C_{2k} > C_{2k-2} > C_2 > C_0$

For $k \in N$ If $q_0 \; q_1 \ldots q_{n\ldots}$ is an infinite sequence of integers $q_i > 0$ for $j > 0$

Let $C_k = (q_0; q_1 \ldots . q_k)$

If $\text{Lt } c_k = \alpha \quad k \longrightarrow \infty$ then $\alpha = (q_0, q_1, q_2 \ldots q_k \ldots)$, Infinite simple continued fractions represent irrationals. Two distinct infinite continued functions represent 2 distinct irrationals.

Let α_0 be irrational

Let $q_0 = [\alpha_0]$

$q_i = [\alpha_i]$

$\alpha_{i+1} = 1/(\alpha_i - q_i)$

$q_0 = [\alpha_0]$

$\alpha_1 = 1 / (\alpha_0 - q_0)$

$q_1 = [\alpha_i]$

$\alpha_2 = 1 / (\alpha_1 - q_1)$

$q_2 = [\alpha_2]$

$\alpha = (q_0; q_1, q_2 \ldots)$

Example let $\alpha_0 = \frac{1 + \sqrt{29}}{2}$

$[\alpha_0] = 3 = q_0$

$\alpha_1 = 1/ \alpha_0 - q_0 = 1/ ((1 + \sqrt{29} / 2) - 3) = 1 / (\sqrt{29} – 5 /2)$

$= (2 / \sqrt{29} - 5) = (\sqrt{29} + 5/2) = 5 + (\sqrt{29} – 5/2)$

$[\alpha_1] = 5 = q_1 \quad \alpha_2 = 1/ (\alpha_1 – q1) = 1 /(\sqrt{29} – 5/2) = 2 /(\sqrt{29} – 5) = \alpha_1,$

Therefore, $1 + (\sqrt{29} /2) = (3 ; 5,5,5,5\ldots\ldots..)$

Periodic Simple Continued Fractions $\alpha = (q_0; q_1, q_2, q_{k-1}, q_k, q_{K+1}, \ldots q_{L+k-1}\ q_k\ q_{K+1}$

$\ldots . q_{L+k-1} , q_k, q_{K+1}, \ldots . q_{L+k-1} ..)$

The smallest k for which $q_k, q_{K+1} \ldots q_{L+k-1}$ repeats itself is called the period

length of

α e.g = 1 + √ 29 / 2 = (3; 5, 5,5,5…)

Quadratic Irrationals

α is a quadratic irrational if it is irrational and a root of $ax^2 + bx + c = 0$ a, b, c, ∈ z

e.g 1 + (√ 29 /2) is a root of x2 – X -7 = 0 a quadratic irrational.

A quadratic irrational is of the form $\alpha = (P + \sqrt{D}) / Q$ P, D, Q integers D > 0

not a perfect square $Q \not\equiv 0$ $Q \mid D - P^2$

-

Algorithm for quadratic Irrational

Let $\alpha_0 = P_0 + \sqrt{D} / Q_0$, $P_0, q_0 \in Z$ $Q_0 \mid D - P_0^2$ $Q_0 \neq 0$ be a quadratic irrational

Let $qi = [\alpha_i]$ $\alpha_j = Pj + \sqrt{D}) / Q_j$

$P_{j+1} = q_j Q_j - Pj$ $Q_{j+1} = D - P_{J+1}^2 / Q_j$

Then α = (q0; q_1, q_2 ……)

The Continued Fraction factoring Method

Let n ∈N not a perfect square Let $C_j = A_j / B_j$ be the jth convergent in the continued fraction expansion of √n Then $A_{j-1}^2 - n B_{j-1}^2 = (-1)^j Q_j$ (j≥ 1) where A_j B_j Q_j were defined earlier. If for some j (even), Q_j happens to be a perfect square

Then $A_{j-1}^2 - n B_{j-1}^2 = m^2$ ∴ n | $A_{j-1}^2 - m^2$ ∴ n | (A_{j-1} + m) (A_{j-1} - m)

If ($A_{j-1} \pm m$, n) > 1 then we have a non-trivial factor of n. In other words

if $A_{j-1} \pm m \neq 0$

or 1 we get a non-trivial factor by finding ($A_{j-1} \pm m$, n)

Example

Let n = 1501, $\sqrt{n} = P_0 + \sqrt{1501} / Q_0$ $P_0 = 0$ $Q_0 = 1$

The Algorithm for the continued fraction expansion of $\sqrt{1501}$gives

$q_0 = [\sqrt{1501}] = 38$

$A_0 = 38$

$B_0 = 1$

$P_1 = q_0 Q_0 – P_0 = 38$

$Q_1 = (1501 – 38^2 /1) = 57$

$q_1 = [\alpha 1] = [38 + \sqrt{1501}/ 57] = 1$

$(q_0 q_1) = 38 + 1/1 = 39$ $A_1 = 39$ $B_1 = 1$

We construct the table

j	0	1	2	3	4
P_j	0	38	19	21	32
Q_j	1	57	20	53	9
q_j	38	1	2	1	7
A_j	38	39	116	115	
B_j	1	1	3	4	

$Q_4 = 3^2 = 9 = m^2$ j = 4

$n = n \mid A_{j-1}^2 – m^2$ i.e. $n \mid 155^2 - 3^2$

i.e n | 158.152 150 | 158.152 (1501, 158) = 79 (1501, 152) = 19

1501 = 79 X 19

We have factored 1501 = 79 X 19 where 79, 19 are primes.

REFERENCES

Hoffstein, Jeffery. Pipher, Jill. Silverman, Joseph. 2010
An introduction to Mathematical Cryptography (Springer, undergraduate text in mathematics) p 1- 187

Mathews,G.B., 1962
Theory of Numbers –Second Edition (Chelsea Publishing, NY)
Binary quadratic forms Analytical Theory p 57 - 102

Mollin, R.A., 2008
Fundamental Number Theory with Applications (Chapman and Hall CRC)
p 201 -242