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, Pollard’s 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
Jsjrdkfqqwslgfhpwifpymwtzlmnrnsjyznqx - 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, \ldots \}

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

a divides b \ (a | b)

If \exists \ k \in Z \ such \ that \ b = ak

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

Facts If \ a | b \ b | c \ a | c \n
\ a | b \ b | a \ \Rightarrow \ a = \pm \ b \n
\ a | b \ a | c \ Then \ a | b \pm 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 \exists \ integer q and r such that

\ a = bq + r \ 0 \leq r < b \quad \text{[The usual quotient and remainder]}

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

\[ a = bq_1 + r_1 \quad 0 \leq r_1 < b \]
\[ b = r_1q_2 + r_2 \quad 0 \leq r_2 < r_1 \]
\[ r_1 = r_2q_3 + r_3 \quad 0 \leq r_3 < r_2 \]
\[ \cdot \]
\[ \cdot \]
\[ r_{k-2} = r_{k-1}q_k + r_k \quad 0 \leq r_k < r_{k-1} \]
\[ r_{k-1} = r_kq_{k+1} \]

The last non zero remainder \( r_k \) 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 \( b \)
\( (a,b) = (b, r_1) = (r_1, r_2). = (r_{k-1}, r_k) = r_k \)

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

Example
\( (2024, 748) = 44 \)
\[ 2024 = 748(2) + 528 \]
\[ 748 = 528(1) + 220 \]
\[ 528 = 220(2) + 88 \]
\[ 220 = 88(2) + 44 \rightarrow \text{GCD} \]
\[ 88 = 44(2) \]

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 \( \exists \) integers \( x \) and \( y \) such that \( ax + by = 1 \)

**Modular Arithmetic**

We say \( a \equiv b \pmod{m} \) \( a, b, m \) integers
If \( m \mid a - b \)
e.g \( 10 \equiv 2 \pmod{4} \) since \( 4 \mid 10 - 2 = 8 \)
\( 15 \equiv 3 \pmod{6} \) since \( 6 \mid 15 - 3 = 12 \)

Some Facts (Results)
If \( a \equiv b \pmod{m} \)
\( c \equiv d \pmod{m} \) then
1) \( a \pm c \equiv b \pm d \pmod{m} \)
\( ac \equiv bd \pmod{m} \)
2) If \((a, m) = 1\) \( \exists \) an integer \( b \) such that \( ab \equiv 1 \pmod{m} \)
In fact, \( a, 2a, 3a \ldots \ldots (m - 1) a \) leave the remainders \( 1, 2 \ldots \ldots (m - 1) \) in
Some order. Therefore, \( \exists \ b \) such that \( ab \equiv 1 \pmod{m} \) \( b \) is called inverse
of \( a \)
i.e., \( b = a^{-1} \pmod{m} \)

Example: \((2, 5) = 1\)
\( b = 3 \) is the solution to \( 2b \equiv 1 \pmod{5} \)
\( 3 = 2^{-1} \pmod{5} \)
\( (4, 15) = 1 \) \( 4 = 4^{-1} \pmod{15} \)
Since \( 4 \ (4) \equiv 1 \pmod{15} \)
We write \( \mathbb{Z}/m \mathbb{Z} = \{0, 1, 2, 3\ldots \ldots (m - 1) \} \)
Remainders on division by m

\[ F_p = \{0, 1, 2, 3 \ldots \ p-1\} \]

\[ F_{p^*} = \{1, 2, 3 \ldots \ldots \ p - 1\} \]

\((Z/mZ)^* = \{a \in Z/mZ \mid (a, m) = 1\}\)

\[ = \{a \in Z/mZ \mid a \text{ has inverse mod } m\} \]

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

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

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

\(\Phi (m) = \# \{a \ : \ 0 \leq a < m \ (a, m) = 1\}\)

\(\Phi (24) = 8\)

For a prime \(p\), \(\Phi(p) = p - 1\). If the letters of the alphabet are assigned the values 0, 1, 2, 3\ldots\ 25

A Shift cipher (or Caesar Cipher) is described by

encryption \(c \equiv p + k \mod 26\)

Decryption \(p \equiv c - k \mod 26\) for a fixed \(k \geq 0\)

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

\(g \equiv g_1 \mod N\)

\(g_2 \equiv g^2 \equiv g g_1 \mod N\)
$g^3 \equiv g^3 \equiv g \; g^2 \mod N$

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

$3^{218} = 3^2 \times 3^{23} \times 3^{24} \times 3^{26} \times 3^{27}$

It is relatively easy to compute $3, \; 3^2, \; 3^2^2, \; 3^2^3, \; 3^2^4 \; \ldots$.

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

<table>
<thead>
<tr>
<th>$i$</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>$3^{2^i}$ Mod 1000</td>
<td>3</td>
<td>9</td>
<td>81</td>
<td>561</td>
<td>721</td>
<td>841</td>
<td>281</td>
<td>961</td>
</tr>
</tbody>
</table>

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

$\equiv 489 \; (\mod \; 1000)$

Much faster than the naïve approach (Totally 11 multiplications)

**Fundamental Theorem of Arithmetic**

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

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

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

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

$p$ prime $a \neq 0 \exists \; b \neq 0 \in \mathbb{Z}/p\mathbb{Z}$

Such that $ab \equiv 1 \; (\mod \; p)$ 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 \mod p

computing inverses in \((\mathbb{Z}/p\mathbb{Z})^{*} = \mathbb{F}_p^{*}\) is easy

**Primitive Roots**

*Fermat’s Little Theorem*

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

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

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

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

By Fermat’s Theorem if \(g \in \{1, 2 (p -1)\}\) \(g^{p-1} \equiv 1 \mod p\)

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

g is called a primitive root mod \(p\). In this case \(\{1, g, g^2 \ldots g^{p-2}\} = \mathbb{F}_p^{*}\)

**Result**

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

(\(\Phi\) 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

\[
\begin{array}{cccccccc}
B & e & d & & s & p & a & c & t \\
66 & 101 & 100 & 32 & 98 & 117 & 103 & 46
\end{array}
\]
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 $B$.

$m_{b-1}\ m_{b-2}\ ...\ m_0\ \Rightarrow \ \text{converted to the corresponding number in binary form}$

$m_{b-1}2^B + m_{b-2}2^{B-2} + m_0 < 2^B$

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

$M = \{m: 0 \leq m < 2^B\}$

$K = \{k: 0 \leq k < 2^B\}$

$C = \{c: 0 \leq c < 2^B\}$

$K$ 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 $B_k$ is chosen such that $B_k \geq 80$ an exhaustive search for the key is considered infeasible. In some cases where meet in the middle collision attacks are available $B_k$ should be chosen $\geq 160$.

Example

Let $2^{159} < p < 2^{160}$ where $p$ is a prime.
Let $K = M = C = \{1, 2 \ldots (p \cdot 1)\} = F_p^*$

Alice and Bob select a key $k$, $1 \leq k < p$

The encryption is done by the function

$$e_k (m) = c \equiv k \cdot m \mod p$$

decryption by

$$d_k (c) = k^1 c \mod p$$

$k^1$ is inverse of $k \mod p$

$$d_k (c) = k^1 c \equiv k^1 km \equiv m \mod p$$

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

$$g^x \equiv h \mod p$$

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

**Asymmetric Ciphers**

As usual we have

$K = \{\text{the space of Keys}\}$

$M = \text{the space of plaintext messages}$

$C = \text{the space of Cipher text messages}$

A Key $K = (K \text{ priv}, \ K \text{ pub})$
Private Key ↓ Public key

for each $K_{pub}$ there is an encryption function $e_{K_{pub}} : M \rightarrow C$

and for each $k_{priv}$ there is a decryption function $d_{k_{priv}} : C \rightarrow M$

such that $d_{k_{priv}}(e_{K_{pub}}(m)) = m$ for every $m \in M$

Note that Alice can send Bob $k_{pub}$ over an insecure communication channel without worrying about Eve decrypting it because it is difficult for Eve to decrypt without knowing the function $d_{k_{priv}}$ 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

$a^x = b \pmod{P}$

$a, b, p$ 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 $e^{th}$ roots is comparatively easy by the following proposition.

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

$\therefore \exists d$ such that $de \equiv 1 \pmod{p - 1} \text{ then } X^e \equiv c \pmod{p}$ has unique solution $X \equiv c^d \pmod{p}$
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 $e \geq 1$ and $N = pq$ and $(e, (p-1)(q-1)) = 1$

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

Example:

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

\[
\begin{array}{c|c}
C & N \\
\hline
17839 & 229.281 \\
\end{array}
\]

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

$17839 d \equiv 1 \pmod{228.280}$

i.e $17839 d \equiv 1 \pmod{63840}$

Solution is $d = 53509 \pmod{63840}$

$x \equiv c^d \equiv 43927^{53509} \equiv 14458 \pmod{64349}$

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 $2^{N-1} \equiv 18152503636 \neq 1 \pmod{N}$

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 $9483 d \equiv 1 \pmod{104728.287116}$
i.e computes $d \equiv 18472798299 \pmod{30069084448}$ and computes the solution $X \equiv 134872^{18472798299} \equiv 2547028026 \pmod{30069476293}$

### RSA Public Key System

<table>
<thead>
<tr>
<th>BOB</th>
<th>ALICE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bob chooses secret primes $p, q$ chooses encryption key $e$ such that $(e, (p-1)(q-1)) = 1$ publishes $N, e$</td>
<td>Alice chooses plaintext $m$ uses Bobs public key $(N, e)$ to compute $C \equiv m^e \pmod{N}$ sends cipher text $C$ to Bob</td>
</tr>
<tr>
<td>Bob solves the congruence $de \equiv 1 \pmod{(p-1)(q-1)}$ computes $m^1 \equiv c \pmod{N}$ then $m^1$ = the plain text $m$</td>
<td></td>
</tr>
</tbody>
</table>

#### 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 $m = 1070777$ $1 \leq m < N$.

Alice computes $C \equiv m^e \equiv 1070777^{948047} \pmod{2430101}$.

$C \equiv 1473513 \pmod{2430101}$ Alice sends $C$ to Bob.

### RSA decryption

Bob knows $(p-1)(q-1) = 1222 \cdot 1986 = 2426892$.

He solves $de \equiv 1 \pmod{(p-1)(q-1)}$ i.e., $948047d \equiv 1 \pmod{2426892}$ and finds
d = 1051235. Then bob computes c^d mod N
i.e. 1473513^{1051235} \equiv 1070777 (mod 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 ∈ N to find primes
p | n = 1, 2 ... k such that n= P_1^{a_1} P_2^{a_2} .... P_k^{a_k} P_1< p_2 < .... P_k
a_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 ≤ 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 ≤ \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 \( r^2 + 2rs + s^2 \geq 4n \)  \( r^2 + s^2 > 2n = 2rs \) which is true

This suggest that we try

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

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 \( x^2 \equiv y^2 \mod n \), If \( x \neq \pm y \mod n \), \( (x \pm y, n) \) will give non trivial factors of \( n \). The running time can be shown to be \( O(n^{1/6}) \)

Example

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

\[
\begin{align*}
25217 + 1^2 &= 25218 \\
25217 + 2^2 &= 25221 \\
25217 + 3^2 &= 25226 \\
25217 + 4^2 &= 25233 \\
25217 + 5^2 &= 25242 \\
25217 + 6^2 &= 25253 \\
25217 + 7^2 &= 25266 \\
25217 + 8^2 &= 25281 = 159^2 \\
25217 &= 159^2 - 8^2 = 167.151
\end{align*}
\]

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 3N + 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^i = a^{(p-1)} ≡ 1 mod p (Fermat’s title theorem)
a^j \equiv a \mod q \text{ since } j \neq 0 \text{ It is unlikely } a^j \equiv 1 \mod q \text{ therefore } P | a^L - 1 \text{ q does not divide by } a^L - 1 \text{ with high probability. But this is good for we can recover } p \text{ by computing } (a^L - 1, N) \text{ [ Note we use q does not divide } a^L - 1 ] \text{ For otherwise } (a^L - 1,N) = N \text{ How can we find such } L ? \text{ If } p - 1 \text{ has small prime factors then } p-1|n! \text{ for not too large values of } N. \text{ So here is the idea for each } n = 2,3 .. \text{ compute } (a^{n!} - 1, N) \text{ We take } a = 2 \text{ in practice } \text{ IF G.C.D=1 we go to next step If somewhere } \text{ GCD = } N \text{ we are unlucky. May be some other a will work. Otherwise we have a nontrivial factor of N. } a^{n!} - 1 \text{ is quite large e.g } 2^{100!} - 1 \text{ is a number greater than the number of elementary particles in the universe. Luckily we don't need } 2^{100!} - 1 (\mod N) \text{ all we need is } 2^{100!} - 1 \mod N. \text{ So we don't need to work with numbers } > N. \text{ Secondly we do need to compute } n! \text{ Assume we computed } a^n \mod N = (a^{n+1})! \mod N = (a^n)^{n+1} \mod N \text{ so we have to raise to the power } n + 1 \text{ the previous step and the fast powering algorithm does it easily } a^n \mod N \text{ can be computed in } 2n \log_2 n \text{ steps. It is possible to compute } a^n \mod N \text{ for reasonably large values of } n. \text{ We use pollards p-1 method to factor } N = 13927189 \text{ starting with } (2^{9!} - 1, N) \text{ } 2^{9!} - 1 \equiv 13867883 \mod 13927189 \text{ (2^{9!} - 1, 13927189) = 1} \text{ } 2^{10!} - 1 \equiv 5129508 \mod N \text{ (2^{10!}-1,N) = (5129508, N ) = 1} \text{ } 2^{11!} - 1 \equiv 4905233 \mod N \text{ (2^{11!}-1,N) = 1} \text{ } 2^{12!} - 1 \equiv 6680550 \mod N \text{ (2^{12!}-1,N) = 1} \text{ } 2^{13!} - 1 \equiv 6161077 \mod N \text{ (2^{13!}-1,N) = 1} \text{ } 2^{14!} - 1 \equiv 879290 \mod N \text{ (2^{14!}-1,13927189) = (879290, 13927189) = 3823} \text{ We have a non-trivial factor of } N = 13927189 \text{ 3823 is a prime Since the other factor of } 13927189 / 3823 = 3643 \text{ which also prime } 13927189 = 3823 \times 3643
The Continued Fraction Method

Finite Continued Fractions

An expression of the form \[ \alpha = q_0 + \frac{1}{q_1 + \frac{1}{q_2 + \frac{1}{\ddots + \frac{1}{q_k}}}} \]
where \( q_i \in \mathbb{R} \) for \( i > 0 \) \( k \in \mathbb{Z} \)

\( k \) a non-negative integer is called a continued fraction.

This is also written as \( q_0 + \frac{1}{q_1 + \frac{1}{q_2 + \frac{1}{q_k}}} \)

or \((q_0 ; q_1, q_2, \ldots, q_k)\)

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

If \( q_i \in \mathbb{Z} \) 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 \( \alpha = (q_0 ; q_1, q_2, \ldots, q_L) \) \( L \in \mathbb{N} \) be a finite continued fraction.

Let \( C_k = (q_0 ; q_1, q_2, \ldots, q_k) \) \( k \leq L \) \( k \in \mathbb{Z} \)

\( C_k \) is called the \( k^{th} \) convergent of \( \alpha \)

\( C_k = \frac{A_k}{B_k} \) where \( A_k \) and \( B_k \) are given by

\[ A_{-2} = 0 \quad A_{-1} = 1 \quad A_k = q_k A_{k-1} + A_{k-2} \]
\[ B_{-2} = 0 \quad B_{-1} = 1 \quad B_k = q_k B_{k-1} + B_{k-2} \]

\[ C_k = \frac{A_k}{B_k} = \frac{q_k A_{k-1} + A_{k-2}}{q_k B_{k-1} + B_{k-2}} \]

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 \( k \in \mathbb{N} \) If \( q_0, q_1, \ldots, q_n \ldots \) is an infinite sequence of integers \( q_j > 0 \) for \( j > 0 \)
Let \( C_k = (q_0; q_1 \ldots q_k) \)

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

Let \( \alpha_0 \) be irrational

Let \( q_0 = [\alpha_0] \)

\( q_i = [\alpha_i] \)

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

\( q_0 = [\alpha_0] \)

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

\( q_1 = [\alpha_1] \)

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

\( q_2 = [\alpha_2] \)

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

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

[\( \alpha_0 \)] = 3 = q_0

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

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

[\( \alpha_1 \)] = 5 = q_1

\( \alpha_2 = 1/(\alpha_1 - q_1) = 1/((\sqrt{29} - 5/2) = 2/(\sqrt{29} - 5) = \alpha_1, \)

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

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

\( q_{k+1} \)

\( \ldots q_{L+k-1}, q_k, q_{k+1}, \ldots q_{L+k-1} \ldots) \)

The smallest \( k \) for which \( q_k, q_{k+1} \ldots q_{L+k-1} \) repeats itself is called the period
length of
\[ \alpha \text{ e.g } = 1 + \sqrt{29} / 2 = (3, 5, 5, 5, \ldots) \]

**Quadratic Irrationals**

\( \alpha \) is a quadratic irrational if it is irrational and a root of \( ax^2 + bx + c = 0 \) \( a, b, c, \in \mathbb{Z} \)
e.g \( 1 + (\sqrt{29}/2) \) is a root of \( x^2 - x - 7 = 0 \) 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 \( Q \neq 0 \) \( Q \mid D - P^2 \)

**Algorithm for quadratic Irrational**

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

Let \( q_i = [\alpha_i] \) \( q_i = P_j + \sqrt{D} / Q_j \)
\( P_{j+1} = q_j Q_j - P_j \quad Q_{j+1} = D - P_{j+1}^2 / Q_j \)

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

**The Continued Fraction factoring Method**

Let \( n \in \mathbb{N} \) not a perfect square Let \( C_j = A_j / B_j \) be the jth convergent in the continued fraction expansion of \( \sqrt{n} \) Then \( A_{j-1}^2 - n B_{j-1}^2 = (-1)^j \) \( Q_j \) (j \( \geq 1 \))

where \( A_j, B_j, Q_j \) were defined earlier. If for some j (even), \( Q_j \) happens to be a perfect square
Then \( A_{j-1}^2 - n B_{j-1}^2 = m^2 \) \( \therefore n \mid A_{j-1}^2 - m^2 \) \( \therefore n \mid (A_{j-1} + m) (A_{j-1} - m) \)

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

<table>
<thead>
<tr>
<th>j</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>P_j</td>
<td>0</td>
<td>38</td>
<td>19</td>
<td>21</td>
<td>32</td>
</tr>
<tr>
<td>Q_j</td>
<td>1</td>
<td>57</td>
<td>20</td>
<td>53</td>
<td>9</td>
</tr>
<tr>
<td>q_j</td>
<td>38</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>7</td>
</tr>
<tr>
<td>A_j</td>
<td>38</td>
<td>39</td>
<td>116</td>
<td>115</td>
<td></td>
</tr>
<tr>
<td>B_j</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>4</td>
<td></td>
</tr>
</tbody>
</table>

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

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

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

$1501 = 79 \times 19$

We have factored $1501 = 79 \times 19$ 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
Binary quadratic forms Analytical Theory p 57 - 102

Fundamental Number Theory with Applications (Chapman and Hall CRC)
p 201 -242