IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 12, Issue 7, July 2023

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 7, July 2023 ||

| DOI:10.15680/IJIRSET.2023.1207213 |

An Algorithm for Large Semi-Prime-Factorization and its Applications to Affine Ciphers

Henry Blankson [1], Rajan Chattamvelli [2]

Vellore Institute of Technology, Tamil Nadu, India[1]

Department of CSE, Amrita Vishwa Vidyapeetham, Amaravati, AP, India [2]

ABSTRACT: This paper proposes a fast algorithm for factorization of very large semi-prime numbers and its applications to Affine Ciphers with a modulus (m), under the assumption that the gcd (A, m)=1. Also considered is the decryption operation in a given Affine Cipher. Although the congruence method guarantees a unique solution, it may not result in an efficient method to find a solution. These have a broad range of applications in network data transfer and secure communications.

KEYWORDS: co-primes, extended Euclidean algorithm, Euler's Phi function, modular arithmetic, substitution cipher..

I. INTRODUCTION

We are living in the digital era where information security plays a paramount role in the daily lives of netizens. It is a well-known fact that data can be securely transmitted from a source to one or more destinations (sinks) with the help of secure encryption and decryption algorithms. Most of the popular algorithms for this purpose use very large prime numbers. Mathematicians have been attempting for centuries to uncover the myth behind prime numbers since they have a unique property, i.e. such numbers are divisible by themselves and by one only [5]. Many researchers have pointed out that prime-number-based encryption is computationally challenging to crack. These cryptosystems are also being combined with other encryption systems like the Rivest-Shamir-Adleman (RSA) algorithms to get hybrid cryptosystems. These innovatively create different cryptographic keys that assist secure transmission of sensitive and confidential data over unsecure computer or wireless networks [8], [9]. In the first two sections, the framework of this problem is recalled and its importance in both number theory and cryptography are correctly are highlighted. The third section is devoted to recalling the mathematical background for the paper. A simple permutation cipher is defined in Section 4. The proposed method is experimentally evaluated in section 5.2 and some useful conclusions are drawn.

The Affine Cipher method in cryptography is an extension of the Caesar Cipher. The algorithm works by encrypting plaintexts with a value and adding it with a shift P to produce the final ciphertext C. This can be symbolically expressed by the congruence relation

$C \equiv m\,P + b \pmod{n}$,
where n is the alphabet size, m and n are relatively prime (decryption will work only if they are relatively prime) and b is the shift counts (which becomes Caesar cipher for m=1). To achieve this, P must be obtained by solving the equation below.
$P \equiv m^{-1}(C - b) \pmod{n}$
Only the null solution exists if the inverse m (mod n) can be expressed as m-1. If m-1 exists, then the decryption process can be carried out [7] .

II. RELATED WORK

The application of fast semi-prime factorization to encrypt and decrypt text data using affine ciphers and the security of affine cryptography are examined in this paper. This is basically based on a large positive integer N=p*q, which the encryption and decryption algorithms use using a pair of public and private keys where p and q are distinct primes. Many other researchers have attempted the same problem by representing the product of two such primes as the sum of

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 7, July 2023 ||

| DOI:10.15680/IJIRSET.2023.1207213 |

four squares. Shor (1997) achieved polynomial time complexity on a quantum computer, while Lenstra Jr. (1987) and Verkhovsky (2011) used modular elliptic equations for this purpose. Montgomery (1992) extended elliptic curve method using FFT for factorisation, while Li (2018) used parallel probabilistic methods. Overmars & Venkatraman (2021) uses the parity property of Pythagorean tuples to factor semi-primes by reducing the search space by half, using the fact that the difference of these two squares is odd. Zilpa (2021) formulates the problem mathematically using roots of cubic equations in which the larger of the unknown prime factors is the variable, and a user-chosen constant (n) decides the gap (difference) between the prime factors p and q. Shumow (2023) presents an analysis of what steps fail in the RSA algorithm when p-1 and q-1 are not relatively prime to the public exponent e, and derives a plaintext recovery algorithm. Zaki et.al. (2023) enhance the wheel factoring technique to improve the execution time. Jun (2023) used a higher-order unconstrained optimization (HUBO) on D-Wave quantum computer for fast prime factorization that can threaten even the RSA cryptosystem.

III. METHODOLOGY

Prime numbers have engrossed most mathematicians and inquiring minds for many centuries. A prime number p can be defined as a positive integer such that $p \geq 2$ and is only divisible by 1 and p. Examples of prime numbers are 2, 3, 5, 7, 11, 13, …….. In other words, p is a prime if and only if p is a positive integer $p \geq 2$ that is not divisible by any integer m such that $2 \leq m < \sqrt{p}$. Otherwise p is called a *composite* number. Also note that the number 1 is neither a prime nor a composite [3]. Large prime numbers (N) can be randomly generated by applying a primality test on the generated integer until a prime is found. This technique called "primality testing problem" (PTP) can be speeded up by checking if N is divisible by each of the primes less than $\sqrt{N}$. On the average, fewer primality tests will be applied to improve its efficiency to O(log(n)) [2].

Prime factorization problem (PFP), also known as prime decomposition, is the process of breaking down a large composite number into a product of smaller prime numbers. Mathematically $n = p_1*p_2*..*p_m$ where each of the p_k are distinct prime numbers (or powers of them) is called m-factor factorization. Factorizing of very large composite numbers is computationally hard [8]. This property of numbers is exploited in cryptography to transmit data in a highly secure way. The particular case m=2 (2 factors) where a composite number is written as n=p*q where p and q are primes is called integer factorization problem (IFP), and n is called a semi-prime number. This problem is most easily solved using Goldbach's conjecture that the sum of two primes (>2) is always an even integer, and the Pythagoreans property by considering a right-triangle with sides sqrt(pq) and (q-p)/2 with hypotenuse (p+q)/2. Modern cryptographic applications use "n" with 200 or more digits that are formed as the product of two very large primes (typically around 100 digits each).

The 2-factor factorization of integers generally reduces an integer N into its simplest factors p and q such that $p \times q = N$. It is computationally hard to practice this fundamental problem in number theory. This implies that factorization of large integers can be used as a safe method for cryptographic, data communications and data storage systems. Identifying innovative methods for this purpose plays a vital role in modern information security [2] .

The Joye-Paillier algorithm [4] involves a sequence of operations that are generated by candidates q and are co-prime with the first small primes p_i. A primality test, denoted by T(q), is applied on each pending candidate until a prime is found. This is a faster alternative. The symbol Π was therefore defined by [2] as the product of the first r primes, not including $p_i = 2$ as

$$\Pi = \prod_{i=3}^{r} p_i, \quad (1)$$

so that Π, being the product of odd integers, is always odd. The prime numbers are generated in a pre-specified interval $[q_{min}, q_{max}]$. In [2], the authors also define the integers b_{min}, b_{max} and v such that:

$$q_{min} \leq (v + b_{min})\Pi, \text{ and } \quad (v + b_{max} + 1)\Pi < q_{max}. \quad (2)$$

The prime integers are generated in a sub-interval:

$$[(v + b_{min})\Pi, (v + b_{max} + 1)\Pi]. \quad (3)$$

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 7, July 2023 ||

| DOI:10.15680/IJIRSET.2023.1207213 |

III. DEFINITION AND THEOREMS

3. Definitions and Theorems

A. DEFINITIONS

Definition 1
Two integers A and B are said to be **co-primes** if gcd (A, B) = 1.

Definition 2:
Let A ≥ 1 and m ≥ 2 be integers. Then A and m are relatively prime if gcd (A, m) = 1. The number Z_m that are relatively prime to m is often denoted by φ(m) [this function is called the Euler's phi-function].

Definition 3:
An integer B ε [1, M−1] is called a ***Multiplicative Inverse*** of an integer A modulo M, if AB ≡ 1 mod M. Such AB is guaranteed to exist when integers A and M are relatively prime. B is called the multiplicative inverse of A and labelled as A^{-1}.

Definition 4:
The number of positive integers less than m>2, which are co-prime of m is called the ***Euler's Phi function***, φ(m).

When an integer *m* has a known prime factorization

$$m = \prod_i q_i^{k_i},$$

φ(m) can be determined as

$$\varphi(m) = \prod_i (q_i - 1) {q_i}^{k_i - 1}. \quad (4)$$

As an example, consider φ(45). Factorize 45 = 3^2 x 5 and apply the above formula to get

$$\varphi(45) = (3-1) \cdot 3^{2-1} \cdot (5-1)^{1-1}$$
$$= 2 \cdot 3^1 \cdot 4 \cdot 5^0$$
$$= 2 \cdot 3 \cdot 4 \cdot 1$$
$$= 24.$$

Hence φ (45) = 24.

Definition 5:
By similar arguments to the above, one can show that A has a multiplicative inverse and it is unique in modulo m. It may also be noted that if $B = A^{-1}$, then $A = B^{-1}$.

B. THEOREMS

Theorem 1:
The congruence Ax = B (mod m) has a unique solution X ∈ Z_m for every B ∈ Z_m, iff

gcd (A, m) = 1.

Assuming the English Alphabets, m = 26. Since 26 = 2 x 13, the values of A ∈ Z_{26} such that gcd (A, 26) = 1 are A = 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23 and 25.

The parameter B can assume any value in Z_{26}. Hence the Affine Cipher has 12 x 26 = 312 possible keys.

Theorem 2:
The integer A has an inverse modulo m if and only if gcd (A, m) = 1.
An astute reader will notice that definitions 3, 5 and Theorem 2 all follow from Theorem 1.

Theorem 3:
Suppose

$$m = \prod_{i=1}^{m} P_i^{e_i}$$

where the p_i's are distinct primes, $e_i > 0$ are integers, and $1 \le i \le n$. Then

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 7, July 2023 ||

| DOI:10.15680/IJIRSET.2023.1207213 |

$$\varphi(m) = \prod_{i=1}^{n}(P_i^{e_i} - P_i^{e_i-1}). \quad (5)$$

An interpretation of this is that the total number of keys in an Affine Cipher over Z_m is $\varphi(m)$, where $\varphi(m)$ is given above.

So, if m = 26 (using lowercase or uppercase English alphabets)
m = 2^1 x 13^1, hence $\varphi(26)$ = (2 – 1) x (13 – 1) = 1 x 12 = 12 elements.

If m = 36 (using lowercase or uppercase English alphabets and numbers from 0 to 9)
m = 2^2 x 3^2, hence $\varphi(36)$ = (4 – 2) x (9 – 3) = 2 x 6 = 12 elements.

Also if m = 60 (using lowercase and uppercase English alphabets and numbers from 0 to 9)
m = 2^2 x 3^1 x 5^1, hence $\varphi(60)$ = (4 – 2) x (3 – 1) x (5 - 1) = 2 x 2 x 4 = 16 elements.

Theorem 4:
Let p be a prime number such that p ∈ Z_m, then

$$\varphi(p) = p - 1. \quad (6)$$

As a matter of fact, Theorem 4 follows from Theorem 3 by simply considering $m=e_1=1$.

Theorem 5:
The gcd of two integers A and B can be written as Ax + By, for some integers x and y, hence

$$gcd(A, B) = Ax + By. \quad (7)$$

Theorem 6 (FERMAT's LITTLE THEOREM):
Let p be a prime number and A be an integer such that A and p are co-prime, then

$$A^{(p-1)} \equiv 1 \ (mod\ p). \quad (8)$$

IV.AFFINE CIPHERS

Cryptography is the study of storing or transmitting private digital data in a protected way. Several mathematical techniques are used for this purpose. It is now-a-days used in all areas of information security. It can also be considered as the art or science of data storage and transmission in a secure way. Data or documents are converted to an encrypted form before transmission or storage. These are particularly difficult to crack without knowledge on the keys and algorithms used. *Cryptanalysis* is the science that is concerned with the methods to break or expose the techniques used in cryptography. *Cryptology* is the study of cryptography and cryptanalysis. Hence the purposes of cryptography in information security are confidentiality or privacy, data integrity, authentication and non-repudiation [1],[6].

The *Substitution Cipher* is a well-known cryptosystem, which has been used for centuries. Puzzle "cryptograms" that appear in some newspapers are examples of it. This cipher is defined as Cryptosystem 2.2. For the substitution cipher, P and C both are assumed to be the 26-letter English alphabet. As encryption and decryption are considered to be algebraic operations, Z_{26} is used in the Shift Cipher. It is reasonable to assume in the substitution cipher that encryption and decryption are permutations of alphabetic characters.

The Affine Cipher is a special case of the Substitution Cipher. Affine Ciphers use a combination of multiplication with addition and modulo m (where m is an integer) to create a more complex exchange [6]. It is also an example of a mono-alphabetic substitution cipher, where the letters of the English alphabet of size 26 is used. One out of the 26! possible permutations of 26 elements is considered for encryption. Affine Cipher as explained by [10] is the combination of multiplicative cipher and Caesar cipher algorithm. The integers correspond to the twenty-six letters as shown in Table 1 below:

Table 1: Integers and their corresponding letters

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
13	14	15	16	17	18	19	20	21	22	23	24	25

The modulo arithmetic is used to transform each integer that a plain-text letter corresponds to. In the Affine Cipher, the encryption function is of the form

$$E(X) = Y = (Ax + B) \bmod 26,$$

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 7, July 2023 ||

| DOI:10.15680/IJIRSET.2023.1207213 |

where A, B are the keys of the cipher and $A, B \in Z_{26}$. A must also be chosen such that A and 26 are co-prime. When m = 26, the co-primes are 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23 and 25
In order to decrypt the cipher text, the following decryption function is used

$$D(Y) = X = A^{-1}(Y - B) \bmod 26,$$

where A^{-1} is the multiplicative inverse of A (modulo 26).
In general, for all affine cipher encryption/decryption, [10] let $P = C = Z_{26}$ and let

$$K = \{(a, b) \in Z_{26} \times Z_{26} : \gcd(a, 26) = 1\}.$$

For K = (a, b), define the encryption function as

$$\mathbf{e_K(x) = (ax + b) \pmod{26},}$$

and the decryption function as

$$\mathbf{d_K(y) = a^{-1}(y - b) \pmod{26}}$$

for $(x, y) \in Z_{26}$.
To launch an affine cipher, pick two values a and b, as explained in [6], and set

$$e_K(m) = am + b \bmod 26.$$

For example, take a = 3 and b = 8 to get the encryption function as

$$\mathbf{e_K(m) = 3m + 8 \pmod{26}.}$$

An astute reader will notice that C corresponds to the number 02. Put this value for m to get $e_K(02) = 3(02) + 8 = 14$, so that C is encrypted as O. To find our decryption function, set

$s = e_K(m)$. Next solve for m in terms of s to get $s \equiv 3m + 8 \pmod{26}$. Therefore, $s - 8 \equiv 3m \bmod 26$, so that

$$3m \equiv s - 8 \pmod{26}.$$

This gives $m \equiv 3^{-1}(s - 8) \pmod{26}$.

The definition of multiplicative inverse of an integer (as defined in ***Definition 3***), shows that the gcd (3, 26) = 1 and also there will exist an x where $3x \equiv 1 \pmod{26}$.

Observe that $(3)(9) = 27 \equiv 1 \pmod{26}$, and so that x = 9. In general, the Extended Euclidean Algorithm is used to get the value of x = 9.
Now take the value of $3^{-1} = 9$, hence

$$m \equiv 3^{-1}(s - 8) \pmod{26} \text{ or}$$
$$m = 9(s - 8) \pmod{26} \text{ to get}$$
$$m = 9s - 72 \equiv 9s + 6 \pmod{26}.$$

This tells us that

$$\mathbf{m = d_K(s) = 9s + 6 \pmod{26}.}$$

The encryption of the letter C gave us O, so the decryption of O will be

$$m = 9(14) + 6 \pmod{26} \text{ or}$$
$$m = 126 + 6 \pmod{26}, \text{ equivalently}$$
$$m = 132 \pmod{26}, \text{ so that}$$
$$m = 2 \pmod{26}.$$

Hence the decryption of the letter O will be C
It is concluded that an affine cipher can be constructed as follows:

4. Choose a and b with gcd (a, 26) = 1
5. Encryption function is $e_K(m) = am + b \pmod{26}$

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 7, July 2023 ||

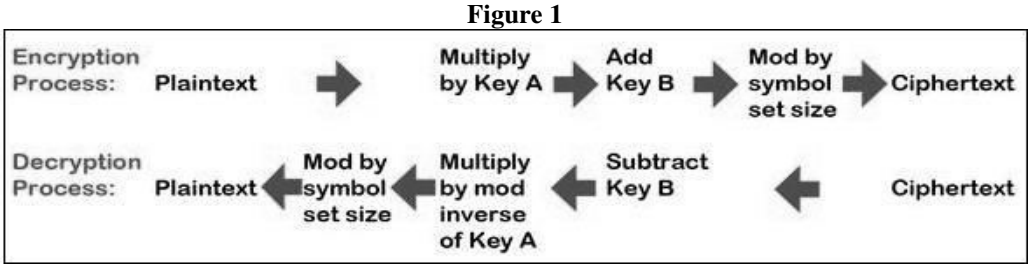
| DOI:10.15680/IJIRSET.2023.1207213 |

6. Decryption function is $d_K(s) = x(s - b) \bmod 26$

where x satisfies $ax \equiv 1 \pmod{26}$.

The basic implementation of Affine cipher as described by [10] is shown in the Figure 1 below:

Figure 1



Encryption: Key Values a=17, b=20

Original Text	T	W	E	N	T	Y		F	I	F	T	E	E	N
x	19	22	4	13	19	24		5	8	5	19	4	4	13
ax+b % 26*	5	4	10	7	5	12		1	0	1	5	10	10	7
Encrypted Text	F	E	K	H	F	M		B	A	B	F	K	K	H

Decryption: a^-1 = 23

Encrypted Text	F	E	K	H	F	M		B	A	B	F	K	K	H
Encrypted Value	5	4	10	7	5	12		1	0	1	5	10	10	7
23 *(x-b) mod 26	19	22	4	13	19	24		5	8	5	19	4	4	13
Decrypted Text	T	W	E	N	T	Y		F	I	F	T	E	E	N

The alphanumeric size of English alphabet A to Z and numbers 0 through to 9 is 36. The encryption of a combination of letters and numbers will consequently replace the 26 to 36 in the encryption and decryption formula stated above. Thus the alphanumeric of size 36 is chosen from the 36! possible permutations of 36 elements. This happens when encrypting passwords that consist of alphabets and numbers. The integers correspond to the thirty-six alphabet and numbers as shown in Table 2 below:

Table 2: Integers with their corresponding alphabets and numbers

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25
0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**			
26	27	28	29	30	31	32	33	34	35			

When m = 36, the co-primes are 1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31 and 35. The simple permutation cipher is not used now-a-days for real-world applications as it is known to be vulnerable to several types of attacks (known plaintext and cryptanalysis).

IV. EXPERIMENTAL RESULTS

An affine cipher tries to improve the problem with the encryption of English language messages where there are only 26 possible ways of encrypting texts. A fast present-day computer can easily crack this easily. This is done by replacing 676 (i.e. 26 x 26) Affine shifts by 26 possible Caesar shifts. Note that 676 is too small for a fast modern computer to crack.

A fast prime-factoring algorithm is proposed below which will enable the factoring of large integers (Int64) and correspondingly, use it in the encryption/decryption of texts in Affine Ciphers.

Parameters: s, Π odd, bmin, bmax, v

Output: a random prime q ∈ [qmin, qmax]

6.

1. Compute $\ell \leftarrow v\Pi$

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 7, July 2023 ||

| DOI:10.15680/IJIRSET.2023.1207213 |

2. Let i ← 0.
3. Randomly choose k ∈ (Z/ΠZ)
4. Randomly choose b ∈ {bmin,..., bmax} and set t ← bΠ
5. Set q ← k + t + ℓ
6. If (q even) then q ←Π − k + t + ℓ
7. If T(q)= false then
(a) Set k ← 2k mod Π
(b) Let i ← i +1
(c) If i < s then go to step 5, otherwise go to step 2.
8. Output q

where T(q) is a testing function. With the above algorithm, co-primes can be generated faster for the encryption and decryption of texts using the Affine Ciphers.

V. CONCLUSION

This paper proposed an efficient and fast prime factorization algorithm that can be used in modular arithmetic during the decryption of ciphers in an Affine decryption process. One of the advantages of using very large prime numbers in Affine Cipher is that it will make it very difficult for attackers to decrypt cipher texts. However, this can be cracked easily when the prime factors are nearby. This helps to close further gaps and weaknesses in RSA like algorithms, thereby making public key cryptography safer. This is a good message for everyone to keep in mind while using cryptography for sensitive data communication.

REFERENCES

1. Babu, S.A.(2017) "Modification of Affine Ciphers Algorithm for Cryptography Password," *Int. J. Res. Sci. Eng.*, 3(2), pp. 346–351.
2. Blankson, H. et.al. (2021) "A symmetric scheme for securing data in Cyber physical systems/IoT sensor-based systems based on AES and SHA256", *Int. J. of Comp. Appl.*, 184(24), 12-17.
3. Clavier,C. and Coron, J. S.(2007) "On the implementation of a fast prime generation algorithm," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 4727 LNCS, pp. 443–449, doi: 10.1007/978-3-540-74735-2_30.
4. da Silva, J.C.L.(2010) "Factoring Semi primes and Possible Implications for RSA", In Proceedings of the 26th IEEE convention of electrical and electronics engineers in Israel, Eliat, 182–183.
5. Gallier, J.(2013) "Notes on public key cryptography and primality testing Part 1 : Randomized Algorithms Miller – Rabin and Solovay – Strassen Tests".
6. Joye, M. and Paillier,P. (2006) "Fast Generation of Prime Numbers on Portable Devices : An Update," pp. 160–173.
7. Jun K. (2023) "HUBO and QUBO models for prime factorization", Quantum Physics, https://arxiv.org/ftp/arxiv/papers/2301/2301.06738.pdf
8. Kaddoura, I. and Abdul-Nabi, S. (2012) "On formula to compute primes and the n th prime," *Appl. Math. Sci.*, vol. 6, no. 73–76, pp. 3751–3757, doi: 10.12988/ams.
9. Kazemi,M., Naraghi, H., and Golshan, H. M.(2011) "On the affine ciphers in cryptography," *Commun. Comput. Inf. Sci.*, vol. 251 CCIS, no. PART 1, pp. 185–199, doi: 10.1007/978-3-642-25327-0_17.
10. Laia, O., Zamzami, E. M., Larosa, F. G. N. and Gea, A.(2019) "Application of Linear Congruent Generator in Affine Cipher Algorithm to Produce Dynamic Encryption," *J. Phys. Conf. Ser.*, vol. 1361, no. 1, doi: 10.1088/1742-6596/1361/1/012001.
11. Lenstra, H.W. Jr.(1987) "Factoring Integers with Elliptic Curves," Annals of Mathematics, 126(2), 649-673. doi:10.2307/1971363
12. Li J.(2018). "A parallel probabilistic approach to factorize a semiprime", American Journal of Computational Mathematics. ; 13:8(2), 175-183.
13. Montgomery,P.L.(1992) "A FFT Extension of the Elliptic Curve Method of Factorization," PhD Thesis, University of California, Los Angeles.
14. Omollo, R., Okoth, A. (2022) "Large semi-primes factorization with its implications to RSA cryptosystems", BOHR international J. of smart computing and information technology, 3(1), 1-8, https://doi.org/10.54646/bijscit.011
15. Overmars, A.; Venkatraman, S. (2021) "New Semi-Prime Factorization and Application in Large RSA Key Attacks". *J. Cybersecur. Priv.*, *1*, 660-674. https://doi.org/10.3390/jcp1040033
16. Rescorla,E.(2001) *SSL and TLS : Designing and Building Secure Systems*, Illustrated. Addison-Wesley.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 7, July 2023 ||

| DOI:10.15680/IJIRSET.2023.1207213 |

17. Rivest, R.L., Shamir, A., and Adleman, L. M.(2019) "A method for obtaining digital signatures and public key cryptosystems," *Secur. Commun. Asymmetric Cryptosystems*, pp. 217–239.
18. Sivananda, L.E., Raghunatha Reddy, V. (2022) Robust Data Security and Authentication Using Multi Level Hybrid Cryptography, Journal of Xidian university, 16(1), 372-376, doi.org/10.37896/jxu16.1/034
19. Shor,P. W. (1997) "Polynomial-time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," SIAM Journal on Computing, 26(5), 1484-1509. doi:10.1137/S0097539795293172
20. Shumow,D.(2023). "Incorrectly generated RSA Keys: "How I learned to stop worrying and recover lost plaintexts", The Computer Journal, bxac199, https://doi.org/10.1093/comjnl/bxac199
21. Stinson, D. R. and Paterson, M. B.(2018) *Cryptography : Theory and Practice*, 4th ed. CRC Press, Taylor & Francis Group.
22. Verkhovsky, B.S.(2011) "Integer factorization of semi-primes based on analysis of a sequence of modular elliptic equations", International Journal of Communications, Network and System Sciences, 4(10), October 2011DOI: 10.4236/ijcns.2011.410073
23. Zaki, A.M., et.al (2023) "Acceleration of Wheel Factoring Techniques", Mathematics,11(5), 1203; https://www.mdpi.com/2227-7390/11/5/1203, https://doi.org/10.3390/math11051203
24. Zilpa, Y.(2021) "About efficient algorithm for factoring semiprime number",Journal of theoretical and computational science, 7(5), Open access, No: 1000P053
25. Zilpa, Y. (2022) "Determination of Efficient Algorithm for Factoring Semiprime Number", Research Highlights in Mathematics and Computer Science, Vol. 1, 16 September '22 , pp. 44-51 https://doi.org/10.9734/bpi/rhmcs/v1/2968C

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.423

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details