A Review of Cryptography Algorithms

Zahra Dorostkar[1] and Ghader Ahmadi Didehbani[2]

[1] Saint Petersburg Electrotechnical University, Ulitsa Professora Popova, 5, St Petersburg, 197022, Russia
[2] APA Moshaver, Tabriz University Main Street 3rd Floor, Central Building, Iran
zdorostkar@stud.etu.ru

Abstract. Security in general has been a very important and basic issue in life of human beings from ancient times. Nowadays, in the information era, information security in particular plays a vital role all around the world. Cryptography is a component which effectively guarantees the security of transmitting information by making information unintelligible for undesirable parties. There are many different cryptography algorithms that the proper selection between them is an important issue. In this article we briefly review all types of cryptography algorithms.

Keywords: Information Technology Security, Cryptography, Encryption, Hashing, Symmetric, Asymmetric, Quantum, Post-quantum

1 Introduction

Cryptography, encryption or enciphering is the algorithm and process of altering a message into another, so called ciphertext, in order not to be understood or changed by an unauthorized person. Likewise, decryption or deciphering is the process of retrieving plain text from the cipher text on the destination side. These algorithms can be categorized in three main groups, including Physical cryptography, Mathematical cryptography and Quantum cryptography, and also an additional group is considered as Post-quantum cryptography. In previous works, some types of algorithms have been considered but there is no comprehensive work which includes every type. In this paper, we review all the main types of algorithms briefly and have an overview of important terms of them such as speed, level of security, effectiveness, attacks, etc.

2 Types of Cryptography

2.1 Physical Cryptography

In this type of cryptography, no mathematical processing is done on the text. The most common method is to move or exchange alphabetic letters (characters) or words, or to hide information inside other information such as an image or audio (Steganography and Watermarking).

The most famous ones are followings:

Atbash : A substitution cipher; Letters of the alphabet are reversed.

ROT13 : A substitution cipher; a letter is replaced with the 13th letter after it; It is often used as a means of hiding spoilers.

Caesar : Shift cipher; Any letter is replaced by a letter with a fixed shift number after that.

Affine : A substitution cipher; Each letter is encrypted with (ax + b) mod 26, a is arbitrary and b is magnitude.

Rail-fence : Zigzag cipher; A transposition cipher; the plain text is written downwards diagonally and upward as well whenever we reach the border, until the whole plaintext is written out. And rewrite it horizontally after all.

Baconian : A 'biliteral' cipher; A method of steganography; Message is concealed in the presentation of text.

Polybius Square : Polybius checkerboard; characters are substituted with pairs of digits.

Simple Substitution : Each unit or letter of plain text is substituted with another letter.

Codes and Nomenclators : It consists of a substitution cipher to change letters of words and codewords to substitute for names or common phrases.

Columnar Transposition : Write the plain text in columns. Then, rearrange the columns according to a key.

Autokey : It is related to the Vigenere cipher, but more secure. Cipher = (Plain+Key) mod26

Beaufort : It is similar to the Vigenere cipher. Cipher = (Key - Plain) mod 26

Porta : It is a polyalphabetic cipher like Vigenere but it only uses 13 alphabets.

Running Key : It is similar to the Vigenere cipher, but the key is a long text which is not repeated.

Vigenère and Gronsfeld : A polyalphabetic substitution cipher; It uses the 'tabula recta' to encrypt the plaintext.

Homophonic Substitution : replaces each letter with a variety of substitutes.

Four-Square : It consists of four 5*5 matrices the upper-left and lower-right matrices are the plaintext, containing a standard alphabet. The upper-right and lower-left are the ciphertext, containing a mixed alphabetic sequence. Split the plaintext into 2 by 2 letters and find the first letter in the upper-left plaintext matrix, the second in lower-right. The row of first and the column of second make the position of first cipher letter, opposite makes second cipher letter.

Hill : Each letter is represented by a number modulo 26, then each block of n letters is multiplied by an invertible $n \times n$ matrix, modulus 26.

Playfair : Encrypts pairs of letters. The key is a 5×5 matrix of alphabets which starts by a key and continues by the rest of the alphabet. The row and column of each two letters shows the substitution cipher letter.

ADFGVX : A fractionating transposition; field cipher; using polybius square; each letter substituted by the same row and column letter.

ADFGX : A fractionating transposition; similar to ADFGVX without numbers in the matrix.

Bifid : A combination of the Polybius square, transposition, and fractionation to achieve diffusion.

Straddle Checkerboard : Monome-dinome cipher; changes alphabetic plaintext into digits and simultaneously achieves fractionation.

Trifid : It combines substitution with transposition and fractionation; similar to Bifid, except that instead of a 5 by 5 keysquare it has a 3 by 3 by 3 key cube.

Fractionated Morse : First converts the plaintext to morse code, then enciphers fixed size blocks of morse code back to letters.

2.2 Mathematical Cryptography

In this type, mathematical algorithms are used for changing information of text or any multimedia such as image or audio signal etc. There are three considerable categories here: *Hashing*, *Symmetric* and *Asymmetric*.

Hashing algorithms include MD2, MD4, MD5, SHA-1, RIPEMD-160, Whirlpool, SHA-2, SHA-3, BLAKE2 and BLAKE3. Symmetric algorithms are DES, Advanced Encryption Standard (AES, Rijndael), MARS, Triple DES (3DES), Educational Data Encryption Standard (E-DES), Blowfish Encryption, SEAL Algorithm, RC2, RC4, RC6, Twofish, Serpent, IDEA, CAST, HiSea and asymmetric algorithms include RSA, ECC, ElGamal Encryption System(DSA), Diffie-Hellman, XTR.

On the basis of the input data, encryption algorithms are classified as block ciphers, in which the size of the block is of fixed size for encryption and stream ciphers in which a continuous stream is passed for encryption and decryption. RC2, AES, DES, RC6 and BLOWFISH are some of the examples of block cipher. In a symmetric algorithm high security can't be achieved as it makes use of the same key for both encryption and decryption, hence asymmetric algorithms are used. It is also known as Public key encryption. [1],[2],[3],[4] A new approach is using chaotic dynamics in cryptography in two ways: To generate pseudo-random sequences, which are used as keystreams to mask the plaintext and corresponds to stream ciphers. To use as initial state and the ciphertext follows from the orbit being generated, in block ciphers. Also they are being proposed for hashing, key-exchange protocols, authentication, etc.

- ❑ **Hash algorithms**

Let ℓ, n be positive integers. We call f a hash function with n-bit output and ℓ-bit key if f is a deterministic function that takes two inputs, the first of arbitrary length, the second of length ℓ-bits, and outputs a binary string of length n. Formally, $H:\{0,1\}^*\times\{0,1\}^\ell\rightarrow\{0,1\}^n$.[5]

Different types of hash functions include: Based on block cipher, Based on modular arithmetic, Based on cellular automation, Based on knapsack problem, Based on algebraic matrices.

MD2 : It generates a 16-byte message for an arbitrary input message. finding a message with a given message digest is in time complexity of O(2^128) and finding two messages with the same message digest is O(2^64).

MD4 : The resulting digest length is 128 bits and the same complexity as MD2.

MD5 : The strengthened version of MD4 where one extra round is added and each round has more operations.

SHA : SHA-0 and SHA-1 have a 160 output size, 512 block size and 80 rounds. In SHA-2 output size is varied from 224 to 512. For the size 224 and 256 of output, block size is 512 with 64 rounds and for output size 384, 512 and others in SHA-2 we have 1024-bit block size and 80 rounds. In SHA-3 there is a fixed number of rounds, 24, for all types. SHA-3 has a similar hash length as SHA-2, the internal state is different and is resistant to threats like length expansion which MD5 and SHA-1 were not resistant to. No attack on it is reported yet.[6]

BLAKE : The HAsh Iterative FrAmework (HAIFA) is an enhanced version of the MD iteration mode and BLAKE uses a simplified version of HAIFA that retains all of HAIFA's desirable properties. BLAKE includes four hash functions: BLAKE-224, BLAKE-256, BLAKE-384, and BLAKE-512. The word length for two first ones is 32 bit, block size 512 bit and salt 128 bit. The next ones have 64 bit wordsize, 1024 bit block size and 256 bit salt. The digest size is 224, 256, 512, 384 bit.[7]

HAVAL : It is very similar to MD5 with these advantages: it uses five nonlinear boolean functions with Strict Avalanche Criterion property. It has 15 different versions by choosing the number of passes 3, 4 or 5 and the digest length 128, 160, 192, 224 or 256 bits. It is 60 % faster than MD5 when 3 passes are required and as fast as MD5 when full 5 passes are required.[8]

RIPEMD : It consists of essentially two parallel versions of MD4, with some improvements to the shifts and the order of the message words.[9]

Whirlpool : It consists of the iterated application of a compression function,based on an underlying dedicated 512-bit block cipher that uses a 512-bit key.[10]

Primary purposes of hash functions are:

- Generation and verification of digital signatures
- Checksum/Message integrity checks
- Source integrity services via MAC
- Derivation of sub-keys in key-establishment protocols & algorithms
- Generation of pseudorandom numbers

- **Symmetric algorithms**

Symmetric keys encryption only uses one key to encrypt and decrypt data. The key should be distributed before transmission between entities.[11]

Below, a comparison between the different symmetric algorithms is presented [12],[13].

Table 1. Symmetric Algorithms

	DES	***AES***	***3DES***	***MARS***	***TEA***
Key Size(bits)	56 + 8 parity	128, 192, 256	112 or 168	128, 192, 256	128
Block Size(bits)	64	128	64	128	64
Round	16	10, 12, 14	48	32	Varies
*Structure**	F	SP	F	F	F
Flexible	No	Yes	Yes	Yes	Yes
Encryption Speed	Slow	Fast	Very Slow	Fast	Slow
*Level of Security***	A	E	A	H	H
*Effectiveness****	Slow in S&H	Ef in S&H	Slow in S	E in S&H	Ef in H
*Attacks*****	B	S	B, KP, ChP	MM	ChP, RK
Algorithm	***Blow- fish***	***SEAL***	***RC2***	***RC4***	***RC6***
Key Size	32-448	160	8,128,64	Varies	128-256
Block Size	64	32	64	40- 2048	128
Round	16	2	16	256	20
Structure	F	Public Key	F	Feistel Stream	F
Flexible	Yes	Yes	Yes	Yes	Yes
Encryption Speed	Fast	Fast	Very slow	Fast	Fast
Level of Security	E	M	G	G	G
Effectiveness	E in S	E in S	Slow in S	E in S	Ef in S
Attacks	D	Not yet	Df, L	BEAST	C
Algorithm	***Two- fish***	***Serpent***	***IDEA***	***CAST***	***HiSea***
Key Size	up to 256	128, 192, 256	128	40 to 128	1-4096 set of int

Block Size	128	128	64	64	64
Round	16	32	8.5	12 /16	4
Structure	F	SP	Lai – Massey(SP)	F	SP
Flexible	Yes	Yes	No	Yes	No
Encryption Speed	Fast	Slow	Slow	Slow	Fast
Level of Security	H	A	H	E	M
Effectiveness	E in S&H	Slow in S&H	Ef in S&H	Slow in S&H	E in S
Attacks	TD	R, L	W	KP, ChP	Not yet
*SP: Substitution-Permutation, F: Feistel **M: Moderate, A: Adequate, G: Good, E: Excellent, H: High ***S: Software, H: Hardware, Ef: Effective, E: Efficient ****B: Brute force, S: Side channel, KP: Known plain text, ChP: Chosen plain text, MM: Meet in the middle, D: Dictionary, Df: Differential, L: Linear, C: Correlation, R: Rectangle algebraic, TD: Truncated differential, W: Weak key, RK: Related key					

The Twofish cipher and the Serpent cipher algorithms have not been patented, and are in public domain.

Main usages of symmetric key algorithms are:

- ➢ Confidentiality is achieved as encryption and decryption is performed using a single key.
- ➢ Integrity and source authentication is achieved by using Message Authentication Codes because the MAC is generated and validated by the same key.
- ➢ Generation of pseudo random numbers [14]

❏ **Asymmetric algorithms**

Asymmetric cryptography, also known as public-key cryptography, uses a pair of keys, one public and one private, to encrypt and decrypt.

RSA: Computing cipher text is in this way: if r and s are prime numbers and a is an integer that has no common divisors with either r or s, then $a^{(r-1)(s-1)} \equiv 1 \mod rs$

Features: Excellent security, Slow.

Possible attacks: Guessing d, Cycle, Common Modulus, Faulty Encryption, Low Exponent, Factoring the Public Key

Elliptic Curve Cryptography(ECC) : The general Weierstrass equation defines a cubic curve E over a field F as the following:
$E: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$
Where $a_1, a_2, a_3, a_4, a_6 \in F$and the discriminant of E is not equal zero. there is a specified point at infinity which is denoted as O. From the general Weierstrass equation, any elliptic curve E in its standard form can be written as: $E: y^2 = x^3 + ax + b$

For cryptography, we need integer points instead of real points. Let GF(p) be the finite field with p elements and E be an elliptic curve. To find all the points in the finite field GF(p), we only need to consider x = 0,1,..., p-1 and take square roots to find the value of y [15].

Features: Excellent security, Fast.

Possible attacks: Side-channel, Backdoors, Invalid curve

ElGamal(DSA) : 1. Obtain the sender's public key(p, α, α^a).
2. Represent the message as an integer m in the range $\{0, 1, . . . , p - 1\}$.
3. Select a random integer k, $1 \le k \le p - 2$.
4. Compute$\gamma = \alpha^k \bmod p$ and $\delta = m \cdot (\alpha^a)^k \bmod p$.
5. Send the ciphertext c = (γ, δ) to the sender.

Features: Efficient security, Fast.

McEliece : 1. Obtain the sender's public key $(\widehat{G}, t)$.
2. Represent the message as a binary string *m* of length *k*.
3. Choose a random binary error vector *z* of length *n* having at most *t* 1's.
4. Compute the binary vector $c = m\widehat{G} + z$.
5. Send the ciphertext *c* to the sender [16].

Features: Excellent security, Fast.

Possible attacks: Brute-force/Unstructured, Structural, Side-channel, Timing, Power consumption

Diffie-Hellman : Diffie-Hellman is based on symmetric key exchange for both encryption and decryption [17]. The simplest implementation uses the multiplicative group of integers modulo *p*, where *p* is prime, and *g* is a primitive root modulo *p*. These two values are chosen in this way to ensure that the resulting shared secret can take on any value from 1 to *p*–1.

Features: Good security, Slow.

Possible attacks: Dictionary, Denial of service, Outsider, Insider, Man in the Middle, Attacks Based on Number Theory, Degenerate Message, Simple Exponents, Simple Substitution, Timing

XTR : XTR stands for 'ECSTR', which is an abbreviation for Efficient and Compact Subgroup Trace Representation. It is a discrete logarithm system. XTR uses a subgroup of the multiplicative group of a finite field $GF(p^6)$ with p^6 elements. The XTR supergroup is of order $p^2 - p + 1$ where p is a prime such that a sufficiently large prime q divides $p^2 - p + 1$. The XTR subgroup has now order q and is as a subgroup of $GF(p^6)^*$ a cyclic group⟨g⟩ with generator g.

Features: Excellent security, Fast.

Possible attacks: Side-channel, Collision

Basic uses of asymmetric algorithms are:

- ➢ Creation of digital signatures
- ➢ To establish/distribute session keys such as in case of TLS protocol

2.3 Quantum Cryptography

In quantum cryptography, a series of photons are used to send a message. If the message in destination is understood by its algorithm, it can be decoded. Otherwise the sender changes the series of photons and resends the message. Quantum cryptography is very expensive and has limited applications. The unit of information in traditional computers is bit which can be 0 or 1 while a quantum state which is named qubit is an element of a finite-dimensional complex vector space (or Hilbert space) H [18],[19].

A qubit can be described by two complex numbers and belongs to the set :

$\{\alpha\,|0\rangle + \beta\,|1\rangle : |\alpha|\ 2 + |\beta|\ 2 = 1, \alpha, \beta \in C\}$

2.4 Post-Quantum Cryptography

The rise of Quantum computers in recent years have given a major setback to classical schemes. RSA and ECC depend on integer factorization and discrete logarithm, which can be easily solved by quantum computers of sufficiently large size running the infamous Shor's Algorithm. Therefore cryptography schemes which are difficult to solve in both traditional as well as quantum computers are needed to be evaluated.

Types of post-quantum cryptography are:

- Public-key encryption:
  - Lattice based Cryptography(NTRU, Ring LWE, BLISS)
  - Code based Cryptography(McEliece, Niederreiter)

- Public-key signatures:
  - Multivariate Cryptography(Rainbow)
  - Hash based Cryptography(Lamport Signature, Merkle Signature)

Table 2. Post-Quantum Algorithms

	Hash-Based	***Code-Based***	***Multivariate-Based***	***Lattice-Based***
*Schemes**	S	S, E, H	S, E	S, E, H, O, I, HE
Practical Speeds	Extremely Fast	Good	Under Test	Under Test
Advantages	Extreme Fast and Modular	Mature and Secure	Fast and Small Key Sizes	Excellent Security Robust Flexible
Disadvantages	Large Footprint Only Signature	Extensive Memory Requirements Variants Proven Insecure	Low Security	Not Fully Tested
* S: Signature, E: Encryption, H: Hash, O: Oblivious Transfer, I: Identity-Based Encryption, HE: Homomorphic Encryption[20]				

3 Conclusion

In this article a comprehensive review of cryptography algorithms has been performed. Three groups of physical, mathematical and quantum have been considered. From a security point of view physical algorithms are not very secure so they are mostly used in watermarking and steganography. Through the previous studies and the result of comparison it has been shown that in the mathematical group, symmetric algorithms are faster than asymmetrics and the most reliable algorithm is AES in terms of speed, complexity, the length of the key, structure and flexibility. On the other hand asymmetric algorithms are significantly more secure. However with the rise of quantum computing all of them are in the risk of being broken. Whereas quantum cryptography is very expensive so a new group of algorithms has been presented for this era as post-quantum algorithms which can be resistant enough.

References

1. O.Abood, S.Guirguis, *A Survey on Cryptography Algorithms*. International Journal of Scientific and Research Publications. 8. 495-516. 10.29322/IJSRP.8.7.2018.p7978.
2. M.Mushtaq et al. *A Survey on the Cryptographic Encryption Algorithms*. International Journal of Advanced Computer Science and Applications. 8. 333-343,2017
3. S.V. Swathi, P.M. Lahari, B.A. Thomas. *Encryption Algorithms: A Survey*, International Journal of Advanced Research in Computer Science & Technology (IJARCST 2016), Vol. 4, Issue 2.

4. C. Burwick and D. Coppersmith, *The Mars Encryption Algorithm*, NIST AES Propos., pp. 1–12, 1999, [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.35.5887&rep=rep1&type=pdf.
5. I. Mironov, *Hash functions : Theory, attacks, and applications Theory of hash functions*, Microsoft Res. Silicon Val. Campus, pp. 1–22, 2005, [Online]. Available: http://research.microsoft.com/pubs/64588/hash_survey.pdf.
6. M. A. Kale and P. S. Dhamdhere, *Survey Paper on Different Type of Hashing Algorithms*, Int. J. Adv.Sci. Res.,vol.3, no.2, pp.14–16, 2018.
7. J.-P. Aumasson, et al. *The Hash Function BLAKE*. 2014.
8. S. Bakhtiari, J. Pieprzyk, and R. Safavi-Naini, *Cryptographic hash functions: A survey,* Cent. Comput. Secur. …, pp. 1–26, 1995.
9. H. Dobbertin, A. Bosselaers, and B. Preneel, *RIPEMD-160: A strengthened version of RIPEMD*, in Fast Software Encryption, 1996, pp. 71–82.
10. Hellman, *The WHIRLPOOL Hashing Function*, Encycl. Cryptogr. Secur., pp. 1384--1385, 2011, [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.529.3184&rep=rep1&type=pdf.
11. T. Nie and T. Zhang, *A study of DES and blowfish encryption algorithms*, IEEE Reg. 10 Annu. Int. Conf. Proceedings/TENCON, pp. 1–4, 2009, doi: 10.1109/TENCON.2009.5396115.
12. S. Charbathia and S. Sharma, *A Comparative Study of Rivest Cipher Algorithms*, vol. 4, no. 17, pp. 1831–1838, 2014.
13. M. Ubaidullah and Q. Makki, *A Review on Symmetric Key Encryption Techniques in Cryptography,* Int. J. Comput. Appl., vol. 147, no. 10, pp. 43–48, 2016, doi: 10.5120/ijca2016911203.
14. A. M. Parker, *Differences between Hash functions, Symmetric & Asymmetric Algorithms*, October 27, 2017, Accessed on: March 25, 2021[online],Available:https://www.cryptomathic.com/news-events/blog/differences-between-hash-functions-symmetric-asymmetric-algorithms
15. I. Setiadi, A. I. Kistijantoro, and A. Miyaji, *Elliptic curve cryptography: Algorithms and implementation analysis over coordinate systems*, ICAICTA 2015 - 2015 Int. Conf. Adv. Informatics Concepts, Theory Appl., no. November, 2015, doi: 10.1109/ICAICTA.2015.7335349.
16. A. J. Menezes; P. C. van Oorschot; S. A. Vanstone. *Chapter 8.4 ElGamal public-key encryption*, Handbook of Applied Cryptography. CRC Press.
17. N. A. Lal, *A Review Of Encryption Algorithms-RSA And Diffie-Hellman,* Int. J. Sci. Technol. Res., vol. 06, no. 07, pp. 84–87, 2017.
18. R. Kumar. *A Survey on Post-Quantum Cryptography for Constrained Devices*. International Journal of Applied Engineering Research. 14. 2608-2615. 2019.
19. D. Bruss, G. Erdelyi, T. Meyer, T. Riege, and J. Rothe, 2007, ACM Computing Surveys, Vol. 39, No. 2, Article
20. R. Asif, *IoT Post-Quantum Cryptosystems for Internet-of-Things : A Survey on Lattice-Based Algorithms*, pp. 71–91, 2021.