International Transaction of Electrical and Computer Engineers System, 2014, Vol. 2, No. 2, 61-66
Available online at http://pubs.sciepub.com/iteces/2/2/3

DOI:10.12691/iteces-2-2-3

Science of Cryptogrraphy

Ogunlewe A. O.[1], Adedoyin M. A.[2,*], Folorunso C.O.[3]

Department of Electronic and Computer Engineering, Lagos State University, Lagos, Nigeria
*Corresponding author: marabote1@yahoo.com

Received February 07, 2014; Revised March 11, 2014; Accepted March 12, 2014

Abstract Cryptography is the science of transforming data using a key such that the data is unintelligible to those who do not have the key. The primitive operation at the disposal of cryptography is encryption. Encryption is used to provide message privacy and integrity. It has helped in the past to ensure secrecy in important communication especially in military and diplomatic sectors. The different algorithm used in cryptography techniques will be highlighted and one of the applications would be presented using a Object Oriented programming language (OOP) to implement.

Keywords: *cryptanalysis, public key cryptography, secret key cryptography, hash function, Digital Signature Standard (DSS), Advanced Encryption Standard (AES), Data Encryption Standard (DES), RSA (Rivest, Shamir, Adleman)*

Cite This Article: Ogunlewe A. O., Adedoyin M. A., and Folorunso C.O., "Science of Cryptogrraphy." *International Transaction of Electrical and Computer Engineers System*, vol. 2, no. 2 (2014): 61-66. doi: 10.12691/iteces-2-2-3.

1. Introduction

The term cryptography is derived from two Greek words: kryptós (hidden) and gráphe (write). When both words are best paraphrased it means "hidden writing". Cryptography could be described as the study of mathematical techniques related to all aspects of information security such that it transforms data (plaintext) to data unintelligible (ciphertext) and vice-versa.

The protection of sensitive communication has been the emphasis of cryptography especially with the advent of Internet that provides essential communication between hundreds of millions of people and is increasingly being used as tool for commerce and e-business.

The internet has made the world a global village where everyone can have access to any information of interest to them. Cryptography allows you to

1. Prove integrity of your data
2. Alert you if the content of your file has changed.
3. Attest to the identity of the users.
4. Secure communication line.
5. Hide important data.

Let us consider one or two typical scenario.

- You have been appointed an Attorney to prosecute someone guilty of a crime where evidences and witnesses must be fiercely protected; hence you must not compromise the evidences or witnesses.
- As a Quality Assurance Manager of a pharmaceutical firm, you need to protect a trade secret to prevent unauthorized person from gaining a competitive edge over your competitors.

Keeping secrets gives one the ability to hide true intentions, gain competitive edge and reduce vulnerability. It had its importance throughout the ages of civilization for one reason or the other. I could recall while growing up my grandfather would speak in a local encrypted language (Ènà) only understood by people of South Western extract of Nigeria.

While cryptography is the science of securing data, cryptanalysis is the science of analyzing and breaking secure communication. Cryptology is a branch of mathematics embracing both cryptography and cryptanalysis. A cryptographic system is a system having a set of algorithms together with the key management processes, that is a well defined computational procedure that takes a variable input and generates a corresponding output as shown in Figure 1

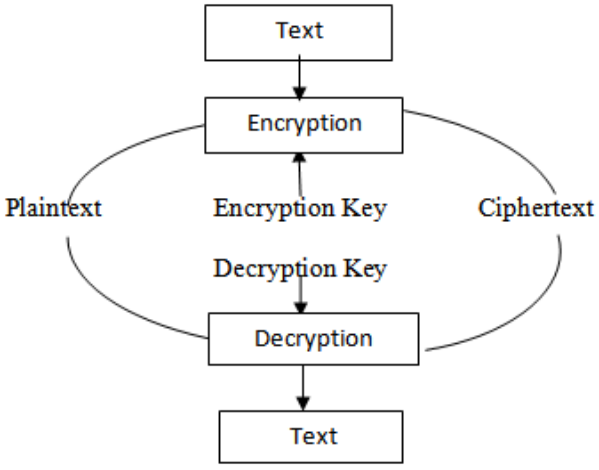

Figure 1. A Typical Cryptosystem

The strength of a cryptographic system is measured in the time and resources required to recover the plain text. The result of a strong cryptography is a cipher text that is

difficult to decipher without having the appropriate decoding tool. Appreciable interests were further developed between 16th and 19th centuries and it was a custom for important personalities to privatize ciphers.

Plaintext denoted by P or M for messages can be a stream of bits, a text file, a bitmap, a stream of digitized voice, a digital video image or a combination of all mentioned. As far as a computer is concerned, the plaintext is simply binary data. The plaintext can be intended for either transmission or storage. In any case, the plaintext P is the message to be encrypted.

Ciphertext is denoted by C and it is assumed also to be a binary data, sometimes the same size as plaintext P or sometimes larger or smaller. However, encryption function (or key) E, operates on P to produce C. Mathematically, this is given as:

$$E(P)=C \tag{1}$$

In the reverse process, the decryption function (or key) D operates on C to produce P:

$$D(C)=P \tag{2}$$

Since the whole point of encrypting and then decrypting a message is to recover the original plaintext, then substituting (1) in (2) yields

$$D(E(P))=P \tag{3}$$

The five requirements of cryptology are:

1. Confidentiality: keep communication private.
2. Integrity: detect unauthorized alteration to communication.
3. Authentication: confirm identity of sender.
4. Authorization: establish level of access for trusted parties.
5. Non-repudiation: prove that communication was received.

These are vital requirements for social interaction on computers, that someone is who he says he is, that someone's credentials whether International passport, driver's license or national identity are valid documents purporting to come from a person actually came from that person.

The main classical cipher types are:

i) Concealment ciphers - is used to hide messages in plain sight. It was reported to have been used in1758 by a prisoner to escape execution by hanging during the time of Oliver Cromwell in England. The next paragraph is an example of a very old concealment cipher, hidden within the message are the instructions to the prisoner on how to escape:

Worthie Sir John: Hope, that is the best comfort of the afflicated, cannot much, I fear me, help you now. That I would saye to you, is this only: if ever I may be able to requite that I do owe you, stand not upon asking me: Tis not much I can do: but what I can do, bee you verie sure I wille. I knowe that, if deathe comes, if ordinary men fear it, it frights not you, accounting is for a high hounour, to have such a rewarde of your loyalty. Pray yet that you may be spare this soe bitter, cup, I fear not that you will grudge any suffereings; onlie if bie submission you can turn them away, tis the part of a wise man. Tell me, as If you can, I do for you anythinge that you can wolde have done. The general goes back on Wednesday. Restinge your servant to command. R.J.

The key to the concealment is, "the third letter after every punctuation mark." and If you follow that key, you will find that the concealed message is:

"panel at east end of chapel slides"

The prisoner requested to go to the chapel to pray before the execution, while the guards stood outside the entrance. After a very long moment the guards went in only to discover he had disappeared.

ii) Substitution Ciphers- as the word implies, a letter or character is systematically used to replace another letter or character respectively.

The sentence **"**cryptography is a way of life" would become "ujqhlgyjshzq ak s osq gx daxw"

Letter	a	b	C	d	e	f	G	h	i	J	k	l	m	n	o	p	Q	r	s	t	u	v	w	x	y	z
Substitute	s	t	U	v	w	x	Y	z	a	B	c	d	e	f	g	h	I	j	k	l	m	n	o	p	q	r

iii) Transposition ciphers- this is one of the oldest form of cipher where the plaintext is rearranged mostly by reversing the order of the text. The sentence "hello this is my world" becomes "ehlol htsi si ym owrdl".

Other well known ciphers include shift ciphers, Hill ciphers, Affine ciphers, Permutation ciphers, Stream ciphers, Vigenere ciphers and RSA just to mention a few.

The threat of data has become obvious especially in the area of communication in a networked environment, ranging from secure commerce and e-payments up to protection of passwords. Cryptography is about communication in the presence of adversary and there has been one central problem limiting the widespread use of cryptography, that problem is key management. The term key refers to a numerical value used by an algorithm to alter information, making that information secure and visible only to individuals who have the corresponding key to recover that piece of information. This problem of key management is solved by public key cryptography.

2. Literature Review

There is no clear year defined but it had its root around 2000B.C in ancient Egypt when hieroglyphics inscription was used to decorate tombs of the deceased not necessarily to hide an information but to make it noble, ceremonial and majestic. It has then been practiced ever since. Some experts have argued that cryptography appeared spontaneously when man communicated his thoughts in speech and writing. Its applications and earlier deployments were mainly diplomatic and designing war battle plans.

One of the oldest known examples is the Spartan scytale. Plutarch tells how Lacedamonian generals exchanged messages by winding narrow ribbons of parchments spirally around a cylindrical staff and the message was then inscribed on the parchment. When the ribbon was unwound, the writing could be read only by the person who had the cylinder of exactly the same size upon which to unwind it such that the letters would reappear in the normal order.

Making secret messages and then sending them on to someone else to figure out is nothing new. The ancient Greeks used ciphers to send secret messages to their armies in the field. Benedict Arnold used a cipher based on a book called Blackstone's commentaries. At a time, Julius Caesar developed a simple method of shifting letters of the alphabet. Today that technique might seem too simplistic to be effective but it served the purpose of concealing the message sent and providing the necessary protection.

The evolution of cryptography continued as Europe refined its practices using new methods, tools and technology throughout the middle age and by late 1800 cryptography was commonly used in the methods of communication between military factions and allies.

Ciphers really came into their own during WWI and WWII. Entire military and government departments were dedicated to the tasks of coming up with new methods of making secret messages. In addition to making secret messages, these offices also had to figure out how to decrypt the enemy's secret messages. It was from that base of intelligence that modern cryptography has come to be. The government soon discovered that, war or no war, they still had to create secret messages.

It is no surprise, then, that new forms of cryptography came soon after the widespread development of computer communications.

3. Methodology

3.1. Types Of Cryptographic Algorithm

There are several ways of classifying cryptographic algorithm and it is based on the number of keys that are employed for encryption and decryption. These algorithms include:

(1) Secret Key Cryptography
(2) Public Key Cryptography
(3) Hash function

3.2. Secret Key Cryptography

The Secret Key Cryptography also called symmetric cryptography or conventional cryptography uses the same key for both encryption and decryption using symmetric cryptography makes it safe to send encrypted messages without fear of interception because an interceptor is unlikely to be able to decipher the message. This algorithm requires that the sender and the receiver agree on a key before securing communication. However, there remains the difficult problem of how to securely transfer the key to the recipient of the message without compromising the intruder.

The security of a symmetric algorithm lies on the key and letting out the key means anyone can decrypt the ciphertext, hence, the key must remain secret as long as the communication must remain between the sender and the receiver.

Secret key cryptography are generally classified as being either stream or block ciphers. Stream ciphers operate on a single bit at a time such that the plaintext and the ciphertext are encrypted differently; it also has a feedback. Block ciphers encrypts one block of data at a time using the same key for each block. In general, when using the same key on each block the same plaintext will always encrypt to the same ciphertext whereas the same plaintext will encrypt to different ciphertext in a stream cipher.

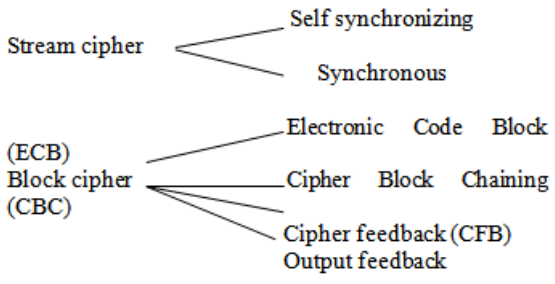

Figure 2. Breakdown of Secret Key Cryptography

Some of the secret key algorithm that are used today include but not limited::

- Data Encryption Standard (DES) designed by IBM in the 70s and adopted by the National Institute for Standards and Technology (NIST) in 1977 for commercial and unclassified Government applications. DES employs 56-bit key that operate on 64-bit blocks and it has a complex set of rules and transformations that were designed specifically to yield fast hardware and slow software implementations.
- Advanced Encryption Standard (AES) – designed by Belgian cryptographer Joan Daemen and Vincent Rijmen in 2001. It uses 128, 192 or 256 bits keys acting on 128, 192 or 256 bits block of data respectively.
- International Data Encryption Algorithm (IDEA) - It is a patented encryption used in PGP software used to replace DES. It uses 128 bit key on 64 bit block data broken into 16 smaller blocks and each has eight round of mathematical functions performed on it.
- Rivest ciphers- designed by Ron Rivest using variable sized keys on a 64 bit block cipher. It had several variants that were released to overcome inherent problems associated with the earlier released versions.
- Blowfish – designed by Bruce Schneier in 1994. It could use up to 448 bit key on 64 bit blocks of data broken down to smaller blocks that goes through 16 rounds of cryptographic functions.
- Twofish - designed by a team led by Bruce Schneier in 1996. It is highly secure and flexible, well- suited for large microprocessors. It uses 128, 192 or 256 bit keys on 128 bit block cipher.
- Camellia - A secret-key, block-cipher crypto algorithm developed jointly by Nippon Telegraph and Telephone (NTT) Corp. and Mitsubishi Electric Corporation (MEC) in 2000. Camellia has some characteristics in common with AES: a 128-bit block size, support for 128-, 192-, and 256-bit key lengths, and suitability for both software and hardware implementations on common 32-bit processors as well as 8-bit processors.
- Secure and Fast Encryption Routine (SAFER) - It is a 40-, 64-, and 128-bit keys acting on 64 bit block cipher. Secret-key crypto scheme designed for implementation in software.
- Kasumi - A block cipher using a 128-bit key that is part of the Third-Generation Partnership Project (3gpp), formerly known as the Universal Mobile Telecommunications System (UMTS). KASUMI is the intended confidentiality and integrity algorithm for both message content and signaling data for emerging mobile communications systems.
- Seed - A block cipher using 128-bit blocks and 128-bit keys. Developed by the Korea Information Security Agency (KISA) and adopted as a national standard encryption algorithm in South Korea.
- Skipjack – It is scheme proposed for Capstone using 80-bit key and 32 iteration cycles per 64-bit block.

3.3. Public Key Cryptography

The primary feature of public key cryptography is that it removes the need to use the same key for encryption and decryption. Prior to PKC, it was impossible to provide key

management large scale networks. With symmetric cryptography, as the number of users increase on the network, the number of keys required to provide secure communication among the users increases rapidly. For 100 and 200 users it will require 5,000 and 20,000 keys respectively for symmetric cryptography. Key management is about generation, transmission and storage of keys and it becomes unwieldy even for relatively small-scale network.

The concept of public key was introduced by Whitfield Diffie and Martin Hellman in 1976 to solve inherent problems associated with management of keys. It was such that each person gets a pair of keys, one called the public key and the other private key. The public key is published (broadcast) while the private key is kept secret. All communications involve only the public key and no private key is ever shared or transmitted making you not worry about the trust on the communication channel against eavesdropper or betrayal..

The only requirement is that public keys are associated with their users in a trusted manner. In other words I can send a confidential message by using the public key but the message can only be decrypted with a private key, which is in the possession of the recipient. Public key encryption can also be used for authentication (digital signatures).

Public key encryption depends on the existence of mathematical functions (one-way) that are easy to compute whereas their inverse function is relatively difficult to compute. An example is the ease of basic mathematical operators such as multiplication and exponentiation compared to relative difficulty of factoring and calculating logarithmic expressions. The mathematical trick of Public key encryption is to find a trap door in the one-way function so that the inverse calculation becomes easy given knowledge of some item of information.

Generic Public key encryption employs two keys related mathematically, although the knowledge of one key does not allow someone to easily determine the other key. One key is used to encrypt the plaintext and the other key is used to decrypt the ciphertext. Because pair of keys is required, this approach is also called asymmetric cryptography. The following are examples of Public key encryption used today:

- **RSA -** Named after three MIT mathematicians that developed it, Ronald Rivest, Adi Shamir and Leonard Adleman. It was the first known algorithm suitable for Public key encryption. It could be used for key exchanges, digital signatures or encryption of small blocks of data that is found in most software products used today.RSA uses a variable size encryption block and a variable size key. RSA is widely used today to secure internet communication tools (browsers, S/MIME, SSL, S/WAN, PGP and Microsoft Outllook), Operating systems (Microsoft, Novell, Apple, Sun and Linux) and hardware (Smartcards, Cell phnes, ATM machines and wireless ethernet cards).
- **Diffie-Hellman (D-H) -** also named after the author, D-H came with their own algorithm and it is used for secret-key exchange only and not for authentication or digital signature.
- **Digital Signature Algorithm (DSA) -** the algorithm specified in NIST's Digital Signature Standard (DSS).
- **ElGamal -** it is a public key algorithm designed in 2001 that can be used for both digital signatures and key exchange. It is based on calculating discrete logarithm in a finite field and not on the difficulty associated with factoring large numbers.
- **Elliptic Curve Cryptography (ECC) -** It was designed for devices with limited computational power or memory such as smartcards and PDAs. ECC algorithm is based upon elliptic curve and it offers a high level of security with small keys comparable to SKC.
- **Cramer-Shoup -** designed in 1998 for IBM by R. Cramer and V. Shoup.
- **Key Exchange Algorithm (KEA) -** It is a variant of D-H proposed as a key exchange method for Capstone.
- **LUC -** A Public key cryptosystem designed in 1994 by P.J. Smith using integer factoring based on Lucas sequence.

3.4. Hash Functions

A one-way hash also called message digest is a function that takes a variable-length string or message and compresses before transforming it to a fixed-length value refer to as hash value. Just as finger prints can be used to identify individuals, harsh values can be used to identify a specific message. It operates by appending a hash value to the message sent such that the recipient uses the same hash function to compare the result with the hash value that was sent by the sender with the message. If the two values are the same the recipient can be rest assured that the message had not been altered, otherwise it is discarded because the message has been altered intentionally or unintentionally.

The hash function, usually an algorithm is a not a secret as it is publicly known. The secrecy of the one-way hash function is the unique orientation of simplex one-wayness, which is quite different from the one-way function used in public key cryptography. In PKC, the security is provided because it is difficult to perform a one-way function on a ciphertext and make it a readable plaintext without knowing the key. However, one-way hash function is never used in reverse mode.

The hashing one-way function takes place without the use of any keys, which means that anyone who receives the message can run the hash value and verify the message integrity. However, if a sender only wants a specific person to be able to view the hash value sent with the message, the value would be encrypted with the key which is referred to as authentication code. The following are hash algorithm commonly used today.

- Message Digest Algorithm (MD) – with many variants developed by Rivest. MD is a series of byte oriented algorithm that produces a 128 bit hash value from an arbitrary-length message designed for systems with limited memory such as smartcards.
- Secure Hash Algorithm (SHA) - approved by NIST. It produces a 160-bit hash value that could be up to 224, 256, 384 or 512 in length.

- RIPEMD - designed by Hans Dobbertin, Antoon Bosselaers and Bart Preneel used to replace 128-bit hash value MD. It wsa optimized for 32-bit processor.
- HAsh of Variable Length (HAVAL) - designed by Y. Zheng, J. pieprzyk and J. Seberry. It provides a hash algorithm with many levels of security and a hash value ranging from 128, 160, 192, 224 or 256 bits in length
- Whirlpool - designed by V. Rijmen and P.S Barreto operates on messages less than 256 bits in length and produces a message digest of 512 bits. It has a high immunity when compared to forms of hash function.
- Tiger - designed by Ross Anderson and Eli Biham in 2001. It is also hghly secure and runs on 64- bit processors.

3.5. Rivest Adi Shamir (RSA)

Diffie and Hellman introduced a new approach to cryptography by throwing open the design for a general purpose encryption algorithm. In 1977 three mathematicians from MIT namely: Ron Rivest, Adi Shamir and Leonard Adleman designed a scheme called RSA(abbreviation of their names) that has now become the most widely accepted and implemented general purpose approach to public key encryption. RSA can be used for key exchange as well as digital signatures and the encryption of small blocks of data.

The security level of RSA is very high when compared to other forms of encryption. RSA mathematical difficulties stems from the ease in calculating large numbers and the finding the prime factors of those large numbers that the algorithm requires. RSA is currently used for many applications like Digital Certificaates, Smartcards and SecureID. This algorithm is considered computationally unbreakable i.e. it would take a very long time to break the code, especially if large keys are used (at least 1024 bits).

Most common algorithm for computing p and q are probabilistic and there are few numbers called Carmichael numbers which certain probabilistic primary algorithms will fail to detect. RSA is much slower than DES and other symmetric cryptosystems. In practice, Alice decides to encrypt a secret message with symmetric algorithm to Bob using RSA encrypted symmetric key. This procedure requires a high level security by using a random number generator for the symmetric key otherwise, Eve(eavesdropper) could bypass the RSA by guessing the symmetric key and then have access to the plaintext.

The following are known problems associated with RSA

1. Mathematically: if anybody finds a way to factor numbers quickly, then this algorithm will become assailable.
2. Timing attacks: A hacker might time key generation process to determine the actual keys.
3. Brute force: One might simply try various keys to see if any match the private key.
4. Bad keys: II f a user picks a small prime number for the private key, it would be easier for a hacker to break their code.

There are 4 stages involved in the deployment RSA cryptosystems. The stages are:

- Finding prime numbers
- Finding the modulo inverse
- Exponentiation
- Decryption

3.5.1. RSA ALGORITHM

The RSA algorithm involves three (3) steps. These are key generation, encryption and decryption. The details of these steps are listed below.

I) RSA KEY GENERATION

i) Pick two large random prime numbers p and q roughly of the same size.

ii) Calculate the RSA modulus n = p*q.

iii) Calculate $\Phi = (p-1)*(q-1)$

iv) Select a random number, e $\in$ N (set of natural numbers) such that $1 < e < \Phi$ and compute the greatest common divisor (gcd) of e and Φ.

Note: the gcd(e, Φ) = 1. Euclid's algorithm is used to find the greatest common divisor of two numbers. The integer e is called the RSA enciphering public exponent.

v) Using the Euclid algorithm, calculate the unique number d called the RSA deciphering private exponent.

d $\in$ N (set of natural numbers) with $1 < d < \Phi$ such that d*emod Φ=1, i.e d is an integer from the quotient (e*d - 1) / [(p-1)*(q-1)].

(vi) The public key is the number pair (n, e) and the private key is (d, n).

Note: Although these values are publicly known, it is computationally infeasible to determine d from n and e if p and q are large enough.

II) RSA Public- Key Encryption

In order to simplify this stage, we assume the plaintext P $\in$ N in numerical form with P < n otherwise the arithmetic modulo n will not be done correctly which prevents the encryption or the decryption process from being unique. Our ciphertext denoted by C.

$$C = P^e \bmod n \tag{4}$$

Where P, e and n are public keys.

III) RSA Public- Key Decryption

To get the original message back, we compute P given by the equation:

$$P = C^d \bmod n \tag{5}$$

Where d and n are the private keys.

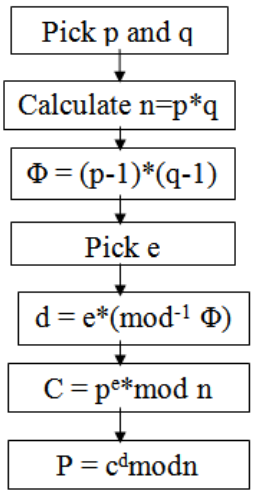

Figure 3. RSA Algorithm design

An example of how this algorithm work is shown below.

1. Select two prime numbers, p =17 and q = 11.
2. Calculate n = p*q = 17*11= 187.
3. Calculate Φ = (p - 1)*(q - 1) = 16*10 = 160.
4. Select e that is a relative prime number to Φ and less than n. i.e 1 < Φ < n (say e = 7)
5. Determine d such that d*emodΦ = 1 and d < Φ. i.e. from ((e*d - 1) / [(p-1)*(q-1)].

d*7mod160 = 1

d = 23.

6. The resulting public key PU = {7, 187} and the private key PR={23, 187}.

If I desire to encrypt a plaintext input of P= 88, then

$$C = P^e \bmod n$$
$$= 88^7 \bmod 187$$
$$= 11.$$

For decryption, we calculate P,

$$P = C^d \bmod n$$
$$= 11^{23} \bmod 187$$
$$= 88.$$

From above, it would be observed that an RSA operation is a modular operation, whether when you are encrypting, decrypting or verifying or signing. This computation is performed by a series of modular multiplication. The speed and efficiency of RSA algorithm has now been enhanced by faster hardware systems and highly robust application software.

APPENDIX I

Euclidean Algorithm

If the prime factorization of two numbers were known, it will be easy to compute their greatest common divisor (gcd). However, for large numbers, it is hard to find their prime factorization. The Euclid's algorithm is a means to find the gcd(a, b) even if their prime factors are not known.

To find gcd (a, b) we divide b into a and write down the quotient and remainder as below.

$a = q_1*b + r_1$
$b = q_2*r_1 + r_2$
$r_1 = q_3*r_2 + r_3$
$r_2 = q_4*r_3 + r_4$
.....
.....
.....
.....
$r_j = q_{r+2}*r_{j+1} + r_{j+2}$
……..
……..
……..
$r_n = q_{r+2}*r_{j+1} + r_{j+2}$
$r_{n+1} = q_{n+3}*r_{n+2} + r_{n+3}$
$r_{n+2} = q_{n+4}*r_{n+3} + r_{n+4}$
$r_{j+n} = q_{j+n+2}*r_{j+n+1} + r_{j+n+2}$

The last non-zero remainder is the gcd. If we work upwards, it would be observed that the last non-zero remainder divides all the previous remainders including a and b. It is obvious that the Euclidean algorithm gives the gcd in a finite number of steps because the remainders are strictly decreasing from one step to another.

Example

Find the gcd (2107, 896)

Solution

2107 = 2*896 + 315
896 = 2*315 + 266
315 = 1*266 + 49
266 = 5*49 + 21
49 = 2*21 + 7
7 = 1*7 + 0

7 is the greatest common divisor.

Note: 7 would divide all the remainders including a and b.

Time Complexity of Euclidean Algorithm

From the previous example on finding the gcd using Euclidean algorithm, it could be shown that $r_{j+2} < ½r_j$

Recall

$r_j = q_{r+2}*r_{j+1} + r_{j+2}$
$r_{j+2} < r_{j+1} < r_j$

at a point of obtaining the gcd,

$r_j = 1*r_{j+1} + r_{j+2}$
$r_{j+2} = r_j - r_{j+1}$
$r_{j+2} < ½r_j$
$r_{j+1} > ½r_j$

It means that the remainder will at least be half of itself in every two steps. Hence, the total number of divisions is at most $2[\log_2 a]$, $\log_2 a$ is the notation for greatest integer function.

Recommendation

Further extension of the matrix to include the 127 ASCII characters.

References

[1] Buchman, J.A., Introduction to cryptography, Springer-Verlag, New York, 2000.

[2] Goldreich, O., Foundations of cryptography, vol. 1, Basic tools, Cambridge University Press, Cambridge, UK, 2001.

[3] Stinson, D.R., Cryptography: Theory and Practice, 2nd Edition, Chapman & Hall/CRC, Boca Raton, FL, 2002.

[4] Fergunson, N. and Schneider, B., Practical cryptography. John Wiley & sons, New York, 2003.

[5] Mao, W., Modern cryptography: Theory and Practice,Prentice Hall PTR, Upper Saddle River, NJ, 2003.

[6] Encarta 2007: cryptography, Microsoft Corporation Inc. 1993-2006.

[7] Yaschenko, V.V., cryptography: An introduction, Student Mathematical library, vol. 18, 2002.