KIU Journal of Humanities Copyright©2019
Kampala International University ISSN: *2415-0843*; 4(2): 37 - 44

An Overview of Public Key Cryptosysems and Application of Residue Number System

JOSEPH B. ESEYIN
University of Jos, Nigeria

KAZEEM A. GBOLAGADE
Kwara State University, Malete, Nigeria

Abstract. The rapid growth in wireless communication system, personal communication system, and smart card technology in our society makes information more susceptible to abuse. The content of the communication may be exposed to an eavesdropper, or system services can be used deceptively. It is vital that these information systems are made secure before these systems are deployed broadly in society. The increasing problem of contraventions in information security has created a demand for serious efforts towards ensuring security of data and information in electronic system communications. The use of these electronic systems for e-commerce, Internet banking, government online services, mobile commerce, Public Key Infrastructure, etc., is dependent on the efficiency of the security solutions. These security concerns are further heightened when resource-constrained environments and real-time speed requirements have to be considered in IT applications. Consequently, these IT security issues have been a subject of intensive research in areas of computing, networking and cryptography.
This paper presents the review of public key cryptosystems and application of residue number system. This public key cryptosystem can be used in wide range of electronic devices, such as Personal Computers, wireless handsets, smart cards, hardware security modules, network appliances, such as routers, gateways, firewalls, and storage and web servers. This paper will examine into details public key cryptography and residue number systems and its application in securing data and information.

Keywords: Public key cryptography, Residue Number Systems, Data Security, Data encryption, Data decryption.

1. Introduction

Communicating securely is becoming more significant as more businesses and transactions are taking place over more and less secured networks. In the early days of the internet, all users knew themselves on the net and all were considered to be honest users. Times have changed however, and the need for encrypting and validating communications is necessary. Providentially, protocols have grown to allow safe and sound exchange of information. Since the inception of written communication effort have been geared up towards the advancement of techniques of secret communication, a science known as cryptography.

Public-key is regularly used to detect a cryptographic process that uses an asymmetric-key pair which makes use of a public-key and a private-key. Public-key encryption uses that key duo for encryption and decryption. The public-key is made public and is dispersed widely and freely. The private-key is never distributed and must be kept secret.

In prearranging a key pair, data encrypted with the public-key can individually be decrypted with its private-key. On the other hand, data encrypted with the private-key can only be decrypted with its public-key. This feature is used to effect encryption and digital signature. Public-key cryptography allows for protected communications, strong authentication, and message integrity.

Residue number system on the other hand is a non-weighted number system. It is different from the weighted number system like binary and decimal number systems. Residue arithmetic operations like addition, subtraction, and multiplication are intrinsically carry-free. Each digit of the result is a function of only one digit from each operand, thereby autonomous of all other digits. This feature helps in substantial improvement on the processing speed, which is the major criterion in cryptographic applications. The rest of this paper is presented as follows; Section 2 provides the basic background information about cryptography. In section 3 we give the fundamental concepts of the representation of numbers in residue number system. Section 4 the application of residue number system in public key cryptography. An in section 5 the paper is concluded.

Before the contemporary age, cryptography concentrated on message confidentiality which is data encryption. This is the translation of messages from a clear form into a meaningless one and back again at the other end, rendering it unreadable by hackers or eavesdroppers without secret knowledge of the key needed for decryption of that message. Encryption tried to ensure secrecy in communications. But recently the field has expanded beyond confidentiality to include techniques for message integrity checking, sender and receiver's identity authentication, digital signatures, interactive proofs and secure computation, among others.

Previously there was a classical cipher which was referred to as transposition ciphers, which reshuffle the order of letters in a message. As an illustration, 'hello world' becomes 'ehlol owrdl' in an inconsequentially trouble-free rearrangement scheme. And subsequently a substitution ciphers, which systematically swap letters or groups of letters with other letters or groups of letters. This can be made simpler with this illustration too; 'fly at once' becomes 'gmz bu podf' by replacing each letter with the one following it in the Latin alphabet. Simple versions of either have never offered much confidentiality from creative opponents since the ciphertexts produced by a classical cipher and some modern ciphers can divulge statistical information about the plaintext, and that information can often be used to crack the cipher. Prior to the early 20th century, cryptography was largely concerned with linguistic and lexicographic patterns. But there was wide-ranging open academic research into cryptography in recent times; it started only in the mid-1970s. And of late, IBM personnel designed the algorithm that became the Federal American Data Encryption Standard; Whitfield Diffie and Martin Hellman published their key agreement algorithm; and the RSA algorithm was in print in Martin Gardner's *Scientific American* column.

And later the stress has loosened, and cryptography now makes wide range use of mathematics, information theory, computational complexity, statistics, combinatorics, abstract algebra, number theory, and finite mathematics.

2. Cryptography

Cryptography is one of the methods used to make sure confidentiality and integrity of information in a communication system are ensured. It resulted from the Greek word kryptos which means secret-writing. Cryptography is the science and art of transforming messages to make them secure and opposed to attack.

Cryptography is generally described as the art and science of scrambling data to prevent

unauthorized access over unsecured transmission channel. Cryptography mostly works on the principle of mathematics that generates different algorithms known as cryptographic algorithm [9]. Cryptographic algorithm is a mathematical function that is used in encryption and decryption method.

Cryptography is a means used to protect information in computing systems. It is used universally on a daily basis. It is used to protect both data at rest and data in motion. Cryptographic systems are an essential part of standard protocols, particularly the Transport Layer Security (TLS) protocol, making it easier to incorporate strong encryption into a wide range of applications.

Data security in modern computing systems is an intricate problem. Network links and remote file system services, which are presumed to be convenient; often make it possible for an intruder to gain access to sensitive data by compromising only a single component of a large system. Because of the dilemma of reliably protecting information, sensitive files are often not stored on networked computers, making access to them by authorized users problematic and putting them out of the reach of useful system services such as backup. Even though, off line backups are themselves a security risk, since they make it difficult to destroy all copies of confidential data when they are no longer needed. In effect, there is fear that computer data are not very private. Thus a situation arises where unadventurous wisdom warns us not to hand over our most important information to modern computers. Cryptographic techniques offer a competent approach for protecting files against illicit access. When correctly implemented and properly applied, modern cipher algorithms (such as the Data Encryption Standard (DES) and the latest IDEA cipher are widely believed amply to render encrypted data unavailable to any foe who cannot supply the correct key.

Internet traffic, which passes information through transitional computers, can be intercepted by a third party. These could be in the form of the following:

- **Eavesdropping:** Information remains intact, but its confidentiality is compromised.
- **Tampering:** Information on transit is changed or replaced and then sent to the receiver.
- **Impersonation:** Information passes to a person who poses as the anticipated recipient.

Impersonation can take two forms:

- **Spoofing:** A person can act as if to be someone else.
- **Misrepresentation:** A person or organization can misrepresent itself

Nowadays cryptography is more than encryption and decryption. It has developed from encrypting files to full scale e-commerce business online, it provides:

- **Confidentiality:** The deterrence of unauthorized leakage of information.
- **Availability:** The stoppage of unauthorized concealment of information or resources.
- **Integrity:** The preclusion of erroneous alteration of information.
- **Authorization:** The process of allowing only approved user's access to sensitive information.

Privacy ensures that only the sender and intended recipient of an encrypted message can read the contents of the message that are transmitted from one place to another and no one can understand it even by any intermediate parties that may have intercepted the data stream.

Non-repudiation provides a method to assure that a party to a transaction cannot falsely claim that they did not participate in that transaction.

2.1 Encryption and Decryption

Encryption is the process of transforming information so it is inarticulate to anyone but the intended recipient. Decryption is the process of decoding encrypted information. A cryptographic algorithm, which can also be referred to as a cipher, is a mathematical

function that is used for encryption or decryption. Typically, two correlated functions are used, one for encryption and the other for decryption. With most modern cryptography, the capability to keep encrypted information undisclosed is based not only on the cryptographic algorithm, which is widely known, but on a key that is essential for use with the algorithm to produce an encrypted result or to decrypt previously encrypted information. Decryption is simple if you have the correct key. Decryption deprived of the correct key will be very hard, if not intolerable.

2.1.1 Symmetric-Key Encryption

With symmetric-key encryption, the encryption key can be considered from the decryption key and viz-a-viz . With most symmetric algorithms, the equivalent key is used for both encryption and decryption, as shown below.

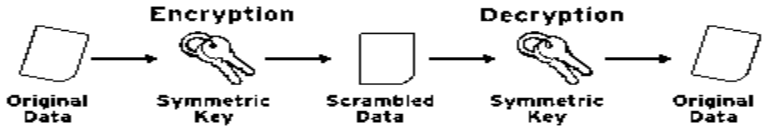

Figure 1.1. Symmetric-Key Encryption

Implementations of symmetric-key encryption can be very proficient, so that users do not experience any major time delay as a result of the encryption and decryption. Symmetric-key encryption also provides a degree of authentication, since information encrypted with one symmetric key cannot be decrypted with a different symmetric key. As long as the symmetric key is kept secret by the two parties using the encrypted message, each of them can be sure that it is communicating with the other as long as the decrypted messages is intact.

Symmetric-key encryption is efficient only if the symmetric key is reserved secret by the two parties. If someone else discovers the key, it affects both confidentiality and authentication. A person with an unauthorized symmetric key can decrypt messages sent with that key, and can also encrypt new messages and send them as if they came from one of the legitimate parties using the key.

2.1.2 Public-Key Encryption

Public-key encryption which is also known as asymmetric encryption involves a pair of keys, a public key and a private key, associated with an entity. Each public key is made available to everyone, and the matching private key is kept secret. Data encrypted with a public key can lonely be decrypted with the matching private key. Encryption shows a simplified view of the way public-key encryption works.

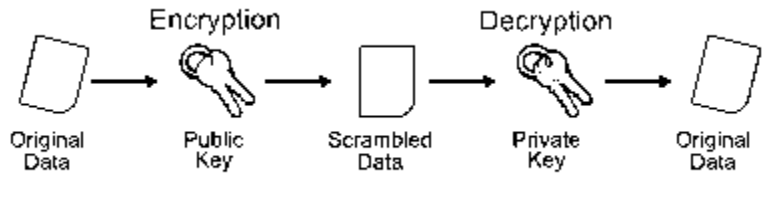

Figure 1.2. Public-Key Encryption

The method shown in Figure 1.2, "Public-Key Encryption" allows public keys to be unreservedly circulated, while only authorized people are able to read data encrypted using the private key. In general, to send encrypted data, the data is encrypted with that person's public key, and the person receiving the encrypted data decrypts it with the equivalent private key.

In relation with symmetric-key encryption, public-key encryption involves more processing and may not be viable for encrypting and decrypting huge amounts of data. However, it is possible to use public-key encryption to send a symmetric key, which can then be used to encrypt additional data.

The reverse of the scheme shown in Figure 1.2, "Public-Key Encryption" also works: data encrypted with a private key can also be decrypted only with the corresponding public key. This is not a suggested practice to encrypt sensitive data, however, because it means that anyone with the public key, which is by definition is made available to all, could decrypt the data. Nonetheless, private-key encryption is beneficial because it means the private key can be used to mark data with a digital signature, a significant condition for electronic commerce and other commercial applications of cryptography.

2.2 Key Length and Encryption Strength

Breaking an encryption algorithm is in essence finding the key to access the encrypted data in plain text. For symmetric algorithms, breaking the algorithm usually means trying to choose the key used to encrypt the text. For a public key algorithm, breaking the algorithm usually means acquiring the mutual secret information between two recipients.

One way of breaking a symmetric algorithm is to simply try every key in the full algorithm until the right key is establish. In case of public key algorithms, since half of the key pair is publicly known, the other half (private key) can be derived using published, though intricate, mathematical calculations. Physically finding the key to break an algorithm is called a brute force attack.
Breaking an algorithm pose the risk of intercepting, impersonating and fraudulently verifying, private information.

The key strength of an algorithm is gotten by finding the fastest method to break the algorithm and comparing it to a brute force attack. For symmetric keys, encryption strength is described in terms of the size or length of the keys used to carry out the encryption. Longer keys generally provide stronger encryption. Key length is measured in bits. An encryption key is considered full strength if the best-known attack to break the key is not faster than a brute force attempt to test every key possibility.

Dissimilar types of algorithms principally public key algorithms may need different key lengths to attain the identical level of encryption strength as a symmetric-key cipher. The RSA cipher can use only a subset of all probable values for a key of a given length, due to the category of the mathematical problem on which it is based. Other ciphers, such as those used for symmetric-key encryption, can use all feasible values for a key of a given length. More possible matching options mean more security. Because it is relatively trivial to break an RSA key, an RSA public-key encryption cipher must have very long key at least 1024 bits to be considered cryptographically strong. On the other hand, symmetric-key ciphers are reckoned to be equivalently strong using a much shorter key length, as little as 80 bits for most algorithms.

3. Residue Number System

A riddle offered in a book written by a Chinese scholar called Sun Tzu in the first century was the first documented materialization of Residue Number System (RNS) representation. The riddle is posed by the following statement:

> We have somethings that the number is not known:
> If this number is counted by threes, it remains 2.
> If counted by fives, the remainder will be 3.
> And if same number is counted by sevens, the remainder is 2.
> Just how many stuffs are there?
> The response is 23.

The mathematical method of obtaining the answer 23 in this riddle from the set of integers 2, 3, and 2 is what was afterward known as the Chinese Remainder Theorem (CRT). The CRT institute an algorithmic solution of decoding the

residue encoded number back into its conventional representation. This theorem is well thought-out to be the foundation in realizing RNSs.

Residue number systems are built on the congruence relation, which can be defined as follows. Two integers a and b are said to be congruent modulo m if m divides exactly the congruence of a and b; it is common, in mathematics tests, to write a ≡ b modulus m to denote this. Thus, for example, 11 ≡ 8 (mod 3),11 ≡ 5 (mod 3),11 ≡ 2 (mod 3. The number m is a modulus or base, and we shall assume that its values rule out unity, which produces only trivial congruencies

If Q and R are the quotient and remainder, correspondingly, of the integer division of a by m that is, a = Q.m + R then, by dentition, we have a ≡R (mod m). The number R is said to be the residue of a with respect to m, and we shall usually denote this by R =|a|m. The set of m smallest values, {0,1,2,...,m−1}, that the residue can assume is called the set of least positive residues modulo m.

Suppose we have a set, {m1,m2,...,mN}, of N positive and pairwise relatively prime moduli [8]. Let M be the product of the moduli. Then every number X < M has an exceptional representation in the residue number system, which is a set of residues {|X|mi : 1 ≤ i ≤ N}. This is assumed to be proved as follows: Suppose X1 and X2 are two numbers with the same residue-set. Thus modulus |X1|mi = |X2|mi, and subsequently |X1 −X2|mi = 0. Consequently X1 − X2 is therefore the least common multiple (LCM) of mi. But if the mi is relatively prime, the LCM is M, and it must be that X1 −X2 is a multiple of M. Therefore, the set {|X|mi : 1≤ i ≤ N} is distinctive and may be taken as the representation of X. We shall write such a representation in the form |x1,x2,...,xNi|, where xi = |X|mi, and we shall indicate the relationship between X and its residues by writing X ~ = { x1,x2,...,xNi}. The number M is called the dynamic range of the RNS, because the numbers that can be represented is M. For unsigned numbers, that range is [0,M −1] .

To make use of the properties of the RNS and carry out the processing in the residue domain, we need to be able to convert easily between the conventional binary representation and the RNS representation. The procedure of conversion from straight representation to RNS representation is named Forward Conversion. Theoretically, this process can be done by dividing the given conventional number by all the moduli and finding the remainders of the divisions. This is the most direct way that can be applied to any general moduli-set.

The universalization arises from the known fact that division of number, that is a power of two, is corresponding to shifting the digits to the right. This property can be used to advance and simplify the forward conversion. The process of conversion from RNS to conventional representation is termed Reverse Conversion. The reverse conversion method is further problematic and presents more overhead in terms of speed and complexity. The algorithms of reverse conversion is based on Chinese Remainder Theorem (CRT) and Mixed-Radix Conversion (MRC).[4] The use of the CRT allows parallelism in the conversion process implementation.

The MRC is an inherently sequential approach. Generally, the understanding of a VLSI execution of a reverse converter is complex and costly. Executing an algorithm by means of parallel distributed arithmetic with no addiction between the arithmetic blocks streamlines the overall design and lessens the complexity of the individual building blocks.

3.1 The Merits of RNS Representation

The importance of RNS representation can be summarized as follows [17,18]:

High Speed: The nonappearance of carry propagation amid the arithmetic blocks results in high speed processing. In conventional digital processors, the critical path is linked with the propagation of the carry signal to the last bit (MSB) of the arithmetic unit. By means of RNS representation, large words are programmed into small words, which outcome is critical path minimization.

Reduced Power: Using small arithmetic units in realizing the RNS processor reduces the switching activities in each channel. This

subsequently results in lessening the dynamic power, since the dynamic power is directly proportional to switching activities.

Reduced Complexity: As the RNS representation encodes large numbers into small residues, the complexity of the arithmetic units in each modulo channel is abridged. This facilitates and simplifies the overall design.

Error Detection and Correction: The RNS is a non-positional system with no dependence between its channels. Thus, an error in one channel does not propagate to other channels. Then, isolating the faulty residues tolerates fault tolerance and facilitates error detection and correction. In fact, the RNS has some embedded error detection and correction features described in.

4. Application of Residue Number System in Public Key Cryptography

As computer arithmetic continues to advance for computation-bound systems, public-key cryptographic processors become progressively more incremental. Researchers are apt to focus their quest for advanced performance on unconventional number system representations. The possibility is not only to further boost up performance but also to investigate new cryptanalytic properties offered by such representations. Among diverse options obtainable, the ancient Residue Number System (RNS) stands out as most prominent of them all.

RNS is appropriate for applications in which addition and multiplication are the major arithmetic operations. Due to its carry-free propagation, RNS has good potential in applications where speed and power consumption is very significant. In addition, the isolation between the RNS-based system designs for public-key cryptography modulo channels facilitates error detection and correction. Residue number system applications are digital signal processing (DSP), digital image processing], RSA algorithms], communication receivers, and fault tolerance. In almost all these applications, exhaustive multiply-and-accumulate (MAC) operations are vital.

A probable application of RNS in DSP is the design of digital filters. Digital filters have diverse usages such as interpolation, decimation, equalization, noise reduction, and band splitting, carrying out the required multiplication and addition operations in the residue domain result in speeding up the system and reducing the power consumption.

Additional conceivable application of RNS in DSP is the Discrete Fourier Transform (DFT) which is a very mutual transform in various engineering applications. Of course, the main operations involved here are addition and multiplication, using RNS in implementing DFT algorithms results in faster operations due to the parallelism in the processing. Also, the carry-free property of the RNS makes it hypothetically very suitable in fault tolerant applications. The RNS has no weight information. Hence, any error in one of the residues does not distress the other modulo channels.

Furthermore, since ordering is not imperative in RNS representation, the defective residues can be discounted and corrected separately. In summary, RNS appears to be good for countless applications that are significant in modern days computing algorithms.

5. Conclusion

As discussed in this paper, RNS is suitable for applications in which addition and multiplication are the main arithmetic operations. Due to its carry-free propagation property, RNS has good potential in applications where speed and power consumption is very crucial. Additionally, the isolation amongst the modulo channels simplifies error detection and correction. Most oftenly these applications require thorough multiply-and-accumulate (MAC) operations. A conceivable application of RNS in DSP is the design of digital filters. Digital filters have diverse uses such as interpolation, decimation, equalization, noise reduction, and band splitting. Carrying out the requisite multiplication and addition operations in the residue domain, results in speeding up the system and reducing the power consumption.

Another possible application of RNS in DSP is the Discrete Fourier Transform (DFT) which is a

very common transform in different engineering applications. The main procedures involved are addition and multiplication, using RNS in implementing DFT algorithms results in faster operations due to the parallelism in the processing. In addition, the carry-free property of the RNS makes it very useful in fault tolerant applications. Nowadays, the integrated circuits are compact, and full testing will no longer be possible. The RNS has no weight information. As such, any error in one of the residues will not affect the other modulo channels. Besides, since ordering is not central in RNS representation, the defective residues can be unessential and adjusted separately. In summary, RNS looks good for many applications that are imperative in modern computing algorithms.

References

Forouzan B. A (2008). Networking and Data Communication (4 Edition)", McGraw Hill Inc. New York.

Chaitanya P. and Sree Y. R. (201) Design of New Security using Symmetric and Asymmetric Cryptography Algorithms." World Journal of Science and Technology. Vol 2. Issue 10. pp. 83-88..

Lai, X. and Massey, J. (1990) A New Block Encryption Standard." Proc. EUROCRYPT 90, 389-404.

N.S. Szabo, R.I. Tanaka, (1967) Residue Arithmetic and Applications to Computer Technology(Mc-Graw Hill, New-York MATH Google Scholar

G. Bi, E.V. Jones, (1988) Fast conversion between binary and Residue Numbers. Electron. Lett. **24**, 1195–1197 Cross Ref Google Scholar

National Bureau of Standards, "Data Encryption Standard." FIPS Publication #46, NTIS, Apr. 1977.

P.V. Ananda Mohan, D.V. Poornaiah, (1991) Novel RNS to binary converters, in Proceedings of IEEE ISCAS, pp. 1541–1544 Google Scholar Ferguson,

Niels; Schneier, Bruce (2003). Practical Cryptography. Wiley. ISBN 0-471-22357-3.

Katz, Jon; Lindell, Y. (2007). Introduction to Modern Cryptography. CRC Press. ISBN 1-58488-551-3.

Menezes, A. J.; van Oorschot, P. C.; Vanstone, Scott A. (1997). Handbook of Applied Cryptography. ISBN 0-8493-8523-7.

IEEE 1363: Standard Specifications for Public-Key Cryptography

Christof Paar, Jan Pelzl (2009) Introduction to Public-Key Cryptography; A Textbook for Students and Practitioners Springer.

Stallings, William (1990). Cryptography and Network Security: Principles and Practice. Prentice Hall. p. 165. ISBN 9780138690175.

Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone (October 1996). Digital Signatures" (PDF). Handbook of Applied Cryptography. CRC Press. ISBN 0-8493-8523-7. Retrieved 2016-11-14

F. J. Taylor, (1984) Residue arithmetic: A tutorial with examples," Computer (IEEE), vol. 17, no. 5, pp. 50-63,

A. Omondi and B. Premkumar (2007) RNS: Theory and Implementation," Imperial College Press 2007, ISBN 978-1-86094-866-4.

N. Szabo and R. Tanaka, (1967) Residue Arithmetic and Applications to Computer Technology," New York: McGraw Hill.

M. A. Soderstrand, W. K. Jenkins, G. A. Jullien, and F. J. Taylor (1986) RNS Arithmetic: Modern Applications in Digital Signal Processing," New York: IEEE Press.