International Journal of Modern Engineering Research (IJMER)
www.ijmer.com Vol.2, Issue.1, Jan-Feb 2012 pp-276-280 ISSN: 2249-6645

A study on algorithms supported by CNG of Windows Operating System

Yasir Ahmad
Manav Bharti University, India

ABSTRACT
Cryptography Next Generation is an encryption Application Program Interface (API) which has been found out by Microsoft, in order to replace CryptoAPI in order to enable developers to add encoding, encryption and authentication to the windows based application that they develop. Cryptography Next Generation supports several algorithms in order to offer security to its users. This paper studies in detail the various algorithms supported by CNG of Windows Vista.

Keywords— Cryptography, Next Generation Cryprography, Windows Operating Systems.

1. CRYPTOGRAPHY NEXT GENERATION (CNG)
CNG was first introduced with Windows Vista. Cryptography Next Generation is extensible at several levels thus enhancing administrators to update, create and use custom cryptography algorithms in AD CS, IP Sec and SSL. One necessary function of cryptography is that it implements the United States government Suite B cryptographic algorithms including algorithms for digital signatures, hashing, key exchange and encryption. The United States NSA (National Security Agency) announced a combined set of asymmetric secret agreement and symmetric encryption also referred to as key exchange, hash and digital signatures functions for future United States government use referred to as Suite B. Suite B is used for the security of information configured as Top Secret and Secret and for private information that was configured Sensitive but uncategorized.

The APIs in Cryptography Next Generation can be used to do the following:

- Utilize and install extra cryptographic providers.
- Decrypt and encrypt data and create hashes.
- Store, create and retrieve cryptographic keys.

Cryptography Next Generation has the following capabilities among its several features:

- In the kernel model support for cryptography for use by boot processes, IP Sec and TLS/SSL. Cryptography Next Generation uses similar API in user and kernel mode for wholly supported features of cryptography. According to Microsoft, not all the functions of cryptography next generations can be referred from kernel mode.
- For organizations the Ability to use their own cryptographic algorithms or standard cryptographic algorithms implementation or to add new algorithms.
- With common criteria needs by storing and utilizing long lived keys in a protective process.
- Support for ECC (Elliptic Curve Cryptography) algorithms needed by United States government's Suite B.
- Support for CryptoAPI 1.0 algorithms and for TPM (Trusted Platform Module) computers which offers major isolation and storage in TPM.
- The capability to exchange the default random number generator by denoting specific random number Generator to use within chosen calls.
- Support for present algorithms supported by Crypto API.

Microsoft recommends that organizations do not deploy Suite B algorithms certificates before those organizations meet the following needs:

- Verify that any occurring PKI enhanced applications can use certificates that depend on cryptography next generation providers of cryptography.
- Verify that logon components of smart card can manage the algorithms of cryptography next generation.
- Before providing any certificates verify that occurring operating systems and CAs are capable to support Elliptic Curve Cryptography algorithms.

Presently organizations that do not have a PKI framework implemented can install a Windows Server 2008 CA once they assure that all occurring applications can support algorithms of Suite B. Organizations acquiring PKI with CAs on previous Windows Server operating systems must add a subordinate CA on a Windows Server 2008 computer. However they must continue using classic algorithms until their occurring CAs have been enhanced. One choice is to add a 2nd PKI and operate cross certification between the 2 CA hierarchies [1].

2. FEATURES OF CNG
Cryptography Next Generation has the following features that vary it from the legacy Crypto API [2].

2.1 Compliance and Certification

Cryptography Next Generation is aiming FIPS (Federal Information Processing Standards) 140-2 level 2 certification together with common criteria evaluation on chosen platforms. Other platforms will meet FIPS 140-2 level 1 certification.

2.2 Auditing

Cryptography Next Generation higher auditing capabilities to meet Common Criteria needs. The events are captured by the KSP (Key Service Provider) in user mode and includes:

- During operations of cryptography failures exist. The operations include decryption, signature verification, encryption, random number generation, encryption, hashing and key exchange.
- During keys testing errors exist. The tests include consistency, verification, parity checks and self tests.
- Destruction, generation, exporting and importing of key pairs.
- Writing and reading of persistent keys to and from the file system.

2.3 Kernel Mode Support

In kernel mode cryptography Next Generation supports cryptography. Kernel mode offers better performance for similar cryptographic features such as IP Sec and TSl/SSl. From kernel mode not all functions of cryptography next generation is being said.

2.4 Agility of cryptography

Cryptography next generation will support agility of cryptography or the capability to deploy new algorithms of cryptography for an occurring protocol such as TLS/SSL (Transport Layer Security/Secure Sockets Layer) or to disable algorithms if vulnerability is found with particular algorithm. This modification to operations of cryptography needs converting most standard cryptographic protocols such as Internet protocol security, S/MIME (Secure Multipurpose Internet Mail Extensions and Kerberos) to permit these protocols to take benefit of new algorithms possible in cryptography next generation.

2.5 Key Storage

For key storage cryptography Next Generation offers a model that supports both cryptography Next generation capable applications. The key storage router denotes the details for key access from both the used storage provider and the application.

3. NEW ALGORITHMS IN CNG

Cryptography Next Generation provides several newer algorithms most probably and notably most necessarily is support for Suite B. Some of the new algorithms of Cryptography Next Generation are:

3.1 RC2 Algorithm

RC2 is a symmetric block cipher configured by Ronald Rivest of RSA [3]. RSA configured RC2 as a direct exchange for DES by developing on the performance and offering a variable key size. RC2 is used commonly in S/MIME secure electronic mail and is referred to be 2 to 3 times as quick as DES. RC2 denotes to use the RC2 encryption algorithm that was developed by RSA Security. RC2 is a block cipher that encrypts data into 64 bits blocks. An encryption algorithm that separates down a message into blocks and encrypts every block is referred to as a block cipher. The key size of RC2 ranges from 8 to 256 bits. In SECURE/SAS a configurable size of key of 40 or 128 bits is used. The RC2 algorithm extends an individual message to a maximum of 8 bytes. RC2 is a proprietary algorithm developed by Data Security Inc. of RSA. RC2 encryption is an alternative to DES (Data Encryption Standard) encryption [4]. RC2 is vastly used algorithm that permits different key lengths but the security experts assume RC2 with little keys to be insecure.

3.2 RC4

RC4 is a stream cipher symmetric key algorithm. Stream ciphers exchange bytes or bits of plaintext streams into bytes or bits of cipher text. The stream cipher benefit is its speed in that only relies on the algorithm and not the performance of acquiring several plain texts. Similarly the stream cipher drawbacks are that it has less diffusion where a cryptanalyst can use techniques of language frequency distribution to separate it which can also lead to message fabrication. In 197 RC4 was developed by Ronald Rivest and kept as trade secret by Data Security of RSA. The below figure shows the RC4 algorithm:

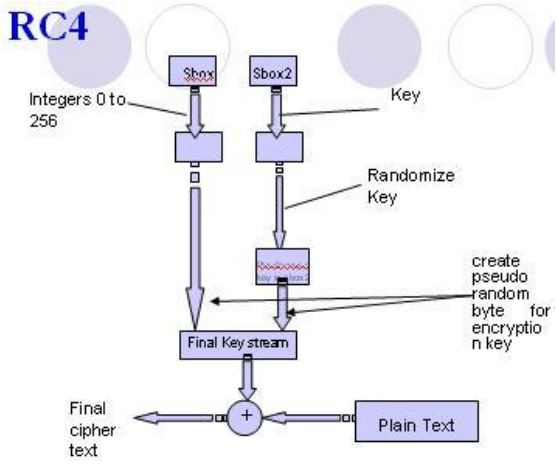

Fig 1: RC4 Algorithm

The RC4 algorithm operates in 2 phases such as encryption and key setup. In the 1st phase the RC4 algorithm uses a variable length key from 1 to 256 bytes to initialize a 256 byte state table Sbox (255). Then the 256 byte array is shuttled by N-number of mixing operations. Thus the key of

RC4 is limited to 40 bits and sometimes used as a 128 bits key. However it has the capability of using keys between 1 and 2048 bits. RC4 is used in several commercial packages of software such as Oracle SQL and Lotus Notes. In the 2nd phase the state table Sbox () is used for subsequent production of pseudo random bytes to produce a pseudo random stream which is XORed with the plain text to give the cipher text.

3.3 Advanced Encryption Standard

The AES (Advanced Encryption Standard) is the recent data security standard referred to as Federal Information Processing Standard 197 (FIPS 197) acquired worldwide by several private and public sectors for protective needs of data storage and secure data communications [5]. The Advanced Encryption Standard is used in several numbers of applications from mobile consumer products to high end users.

In 2001, NIST standardizes the symmetric key algorithm of Advanced Encryption Standard algorithm. The Advanced Encryption Standard denotes the Rijndael algorithm that can access 128 bits of data blocks using keys of 128-, 192- or 256 bit length. The Advanced Encryption Standard encipher exchanges data to an unintelligible form using the cipher key and the Advanced Encryption Standard decipher exchanges the cipher text back to plain text using similar cipher key. In Advanced Encryption Standard (AES) similar key is used for both decryption and encryption. Advanced Encryption Standard decryption and encryption are concerned on 4 various transformations applied again and again in a specific input data consequences and the data flows of decryption and encryption are not similar. The Advanced Encryption Standard also denotes an expansion key module to distribute keys for several iterations of the AES algorithm. The number of iterations of the Advanced Encryption Standard algorithm will vary depending on the input key length [6]. The below figure shows the AES diagram:

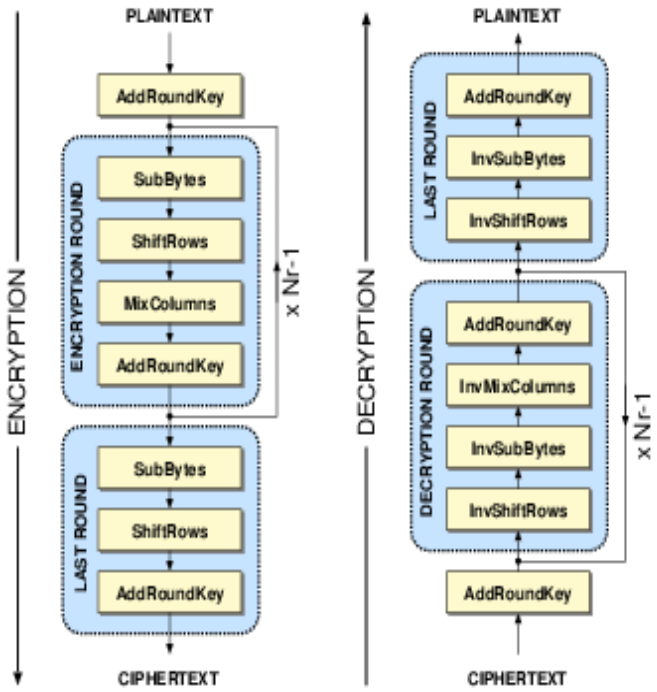

Fig 2: AES

Normally the Advanced Encryption Standard has 3 sizes of blocks such as AES-128, AES-192 and AES-256 bits [7]. From actual data to encrypted data the entire process consists 1 initial round,r-1 standard rounds and 1 final round. The major transformations consist of the following sections:

- Shift Rows: The input bytes are organized into 4 rows. Then according to its row value every row is rotated with a predefined step.
- Sub Bytes: By using a special design substitution box S (box) an input block is transformed byte by byte.
- Add Round Keys: The input block is XORed with the key is that round.
- Mix Columns: By using polynomial multiplication over GF (28) per column basis the 4 row structure which is organized is then transformed.

In the beginning operation there is one round Add Round Key operation and the standard round involves all 4 operations above. And the Mix Columns operation is removed in the final round operation while the other 3 operations remain. On the other hand for decryption the inverse transformations are applied. For quick implementation the round transformation can be parallelized. The entire block encryption is divided into various rounds. The design supporting AES-128 standard consists of 10 rounds.

3.4 Data Encryption Standard (DES)

Data Encryption Standard is the most known block cipher symmetric key which is recognized worldwide and it sets anterior in the middle 1970sas the first modern algorithm based on commercial grade with wholly and openly specified details of implementation [8]. It is defined by the FIPS 46-2 American Standard. The Data Encryption Standard is similar to 2 general concepts such as Feistel ciphers and product ciphers. Each cipher consists of iterating operation rounds or similar consequences operations. The product cipher's basic idea is to construct a composite encryption function by composing many easy operations that provides consequently but singly insecure protection. Basic operations consist of translations, linear transformations and transpositions, simple substitutions and modular multiplication.

A substitution permutation network is a product cipher consisting of several steps each consisting permutations and substitutions.

In a manner more than 2 transformations is integrated by product cipher enhancing that the out coming cipher is more protective than individual elements.

A block cipher consisting of internal function sequential repetition is an integrated block referred to as round function. The parameters consists of the block bit size n, r number of rounds, the Input key K bit size k from which r sub keys Ki from which r sub keys Ki are derived. The below figure shows the DES Algorithm:

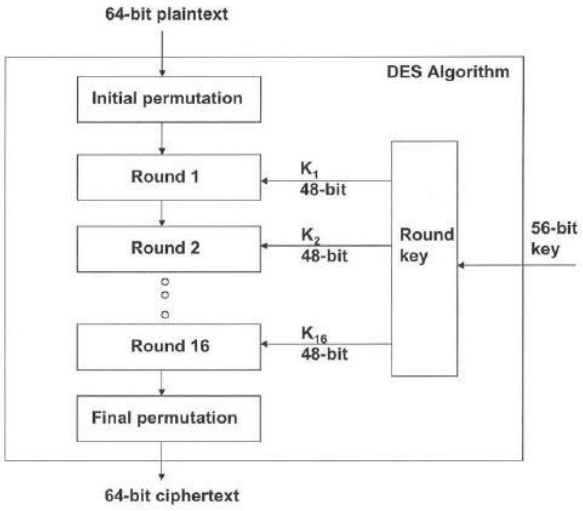

Fig 3: DES Block Diagram

Data Encryption Standard needs a secret key that is 64 bits big but only 56 of those bits are actual key bits the remaining 8 bits are parity bits that assures the internal consistency of every byte of the key [9]. The Data Encryption Standard algorithm involves 16 rounds each one of which uses a varied 48 bit key to work its wonders. The actual 56 bit key is transformed into sixteen 48 bit keys as follows:

- The 56 bits of the key are permuted resulting in two 28 bit values the right hand key source and left hand key source.
- To acquire the key for every round the right hand key source and the left hand key source are shifted circularly each to one or two bits gaining a new right hand and left hand key source. The present round's key is acquired by operating a permutation on the integration of the present left hand key source and the present right hand key source gaining a 48 bit round key.

Data Encryption Standard is a complex algorithm. After the key for every round has been computed the real matter initiates. For CBC Mode every block is XOR'd with the past block's cipher text or for the 1st block with the IV. The XOR'd output is permuted and then categorized into a right hand half and a left hand half. The round key and the right hand half are used as the inputs to a complex numeric evaluation and its result is then XOR'd with the left hand half. The XOR'd output becomes the new right hand half, the previous right hand half becomes the new right hand half and the next round initiates. After these 16 rounds the final right hand and left hand half are concatenated and swapped, once gain permuted and the cipher text occurs. The above described steps are shown in the below figure:

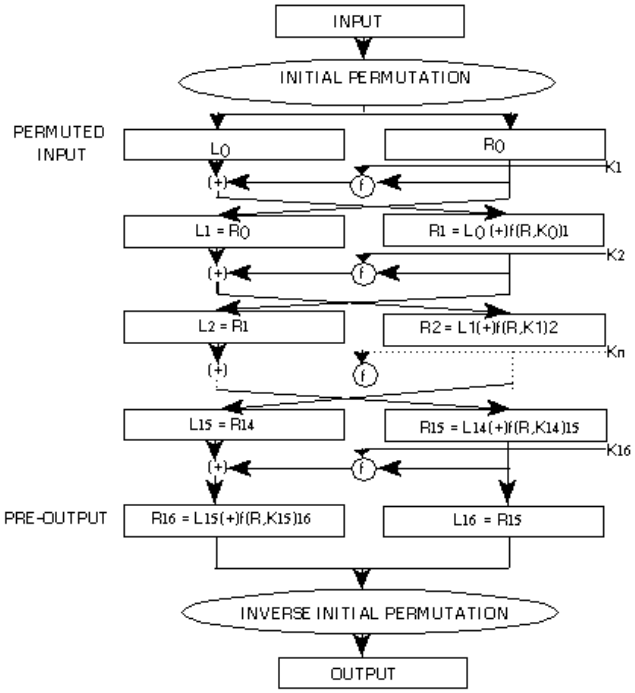

Fig 4: DES Algorithm

3.5 MD2, MD4 and MD5 Hash Functions

MD2, MD4 and MD5 are one way hash functions which were established by Ron Rivest of RSA Data Security Inc. The MD stands for Message Digest [10]. These Algorithms are described in many internet RFCs which also consist of source

code of C language.

In 1989 Message Digest 2 hash algorithm was developed by Ronald Rivest to offer a secure hash function for 8 bit processors. MD2 pads the message so that its length is a multiple of 16 bytes. Then it computes a 16 byte checksum and adds it to the end of the message. Then the 128 bit message digest is produced by using the whole actual message along with the appended checksum. Cryptanalysts Attacks occurs against the MD2 algorithm.

Ronald Rivest developed Message Digest 4 algorithm in 1990 to support 32 bit processors and increase the security level. This developed algorithm is referred to as MD4. It first enhanced the message to assure that the message length is 64 bits smaller than a multiple of 512 bits. Then the MD4 algorithm processes 51 bit message blocks in 3 rounds of computation. The final output is a 128 bit message digest. Many mathematicians have published document papers errors in the full version of MD4 as well as inappropriate Message Digest 4 versions.

Similarly Ronald Rivest established the next version of the Message Digest algorithm in 1991 referred to as MD5. It also processes 512 bit message blocks but it uses 4 varied computation rounds to generate a digest to similar length as the MD4 and MD2 algorithms (128 bits). Message Digest 5 has similar needs of padding as Message Digest 4 and the length of the message must be 64 bits less than a multiple of 512 bits.

Message Digest 4 implements extra features of security that lowers down the message digest production speed essentially. Presently the cryptanalysts attacks describes that the Message Digest 5 protocol is concerned to collisions making it not a one way function [11].

3.6 Secure Hash Algorithm

SHA-1 Secure Hash Algorithm is another hash function which is also referred to as SHS (Secure Hash Standards) which was established by National Security Agency and National Institute of Standards and Technology and is used in government process of United States [12]. It can generate a 160 bit hash value from an arbitrary string length. Secure Hash Algorithm is structurally common to MD5 and MD4. Although it is about 25% slower than MD5 it is much more protective. It generates messages digests that are 25% higher than those produced by the Message Digest Functions making it more protective against attacks than Message Digest 5[13].

4. CONCLUSION

Cryptography is the science of Information security. The algorithms of cryptography are one of the main components in offering the mechanism of computer security. The cryptographic next generation offers exchange for the old API cryptography. BCrypt and NCryp are the sub divisions of cryptography next generation which offers low level primitives of cryptography. The next generation cryptography offered by Windows makes use of several cryptographic algorithms in order to: 1) accomplish key management through quantum cryptography; 2) ensure that Elliptic Curve usage is as quicker and more portable than present asymmetric algorithms; 3) To establish cross web certification quicker several suite are viewed and; 4) finally move word to word suits of standardization to handle the implementation quality of the cryptographic algorithm in electronic mail at various security levels and authentications of cross web.

REFERENCES

1) Price J A, Price B and Fenstermacher S, *Mastering Active Directory for Windows Server 2008, John Wiley & Sons, New York, p 11-40, (2008).*
2) Komar B, *Windows Server® 2008 PKI and Certificate Security, O'Reily Media Inc, USA, (2008).*
3) Burnett M and Foster J C, *Hacking the code: ASP.NET web application security, Syngress, USA, p 165, (2004).*
4) SAS, *SAS 9.2 Language Interfaces to Metadata, SAS Institute Inc., USA, p 31, (2009).*
5) Saadi L, *Stealth Ciphers, Trafford Publishing, Canada, (2004).*
6) Malepati H, *Digital Media Processing: DSP Algorithms Using C, Newns, USA, p 37,(2010).*
7) Flynn M J and Luk W, *Computer System Design: System-on-Chip, John Wiley & Sons, New Jersey, p 251, (2011).*
8) Patel D R, *Information Security: Theory And Practice, Prentice Hall, New Delhi, p 47, (2008).*
9) Frankel S, *Demystifying the IPsec puzzle, Artech House Inc., USA, p 70, (2001).*
10) Hughers L J, *Actually useful Internet security techniques, New Riders Publishing, USA, p 55, (1995).*
11) Stewart J M, Tittle E and Chapple M, *CISSP: Certified Information Systems Security Professional Study Guide, John Wiley Publishing, USA, p 416, (2011).*
12) Stanger J M, Lane P T and Crothers T, CIW: *security professional: study guide, John Wiley & Sons, USA, p 71, (2002).*
13) Singh A and Singh B, *Identifying Malicious Code Through Reverse Engineering, Springer, USA, p 68, (2009).*