Encryption Implementation Paradigm for Digital Resource Management–An Overview

Igboji, Kingsley O*. and Ugwu Gabriel E.

Department of Computer Science, Ebonyi state University – Abakaliki.

E-mail: otubok@yahoo.com, ugwugabrielevo@yahoo.co.uk

ABSTRACT

Encryption is a process that "scrambles" data using sophisticated mathematical equations in order to protect it and keep it private. This process transforms or encodes data in any form such as text, audio, video, graphics etc into another form it will be difficult to understand or interpret. Frequent illegal retrieval and utilization of digital resources as enumerated above arouse the quest for a competent security artifact to eradicate the menace. Encryption key is not mere strings of text like passwords but are essentially blocks of gibberish, thus requires a safe means to pass the key across to end users. Implemented algorithms encrypts original piece until interested users meet certain obligations before access is granted with a decipher key. Research over the years adjudged this approach as a well structured routine in managing digitally embedded resources. A scenario facilitated by utilizing IP authentication, digital certificate, signature and watermarking mechanisms to abate the rake been meted on digital resources. Encryption ostensibly creates a paradigm driven by evolving technological world.

Keywords: encryption, paradigm, watermark, symmetric, asymmetric, cryptography,

INTRODUCTION

Encryption is a process that "scrambles" data using sophisticated mathematical equations in order to protect it and keep it private. In very general terms, encryption algorithms convert or transform human readable data of any form into encrypted or encoded data. To make readable again, requires a technical measure known as decryption through a corresponding decipher key. If the decryption key is given only to authorized parties and if the encryption algorithm used is sufficiently strong, unauthorized access to the data by the casual user is completely prevented.

CONCEPTUAL OVERVIEW

Over the years, innovative ways to search and share digital contents emerged. This undoubtedly created loop holes in regulating access to intellectual properties. Hawa (2008), the emergence of peer-to-peer (p2p) networks with distributed computing architecture made end systems equal (both acting as client and server). Encryption technology is used to protect data and works transmitted over computer networks (such as e-mail and database information), or more broadly in connection with other information delivery systems, including telephone, satellite and cable communications.

But, the whole point of encryption is that an enciphered work cannot easily be manipulated without authorization. Essentially, digital piracy ensued given the ease with which copying and sharing files on the Internet are done (Frattolillo and Landolfi, 2008). In their views, Einhora and Rosenblatt, (2005) strongly established the fact that peer-to-peer networks facilitated illegal sharing of mostly music and videos files. Encryption keys are however not mere strings of text like passwords but are essentially blocks of gibberish, thus requires a safe means to pass the key across to end users. Of course, if you have a safe way to share the key, you probably don't need to be using encryption in the first place.

Apparently, the key issue that distinguishes an analysis of copyright and other forms of intellectual property is that the products involved can be non-rival. This means that multiple consumers can consume or use the product at the same time. For non-rival goods, the price to an additional consumer should be low or zero, since the marginal cost is low or zero (Liebowitz, 1985). He further asserts that copyright allows copying exceptions.

The Paradigm of Encryption Algorithm

Generically, encryption algorithms may be characterized either as “secret key” encryption often called “symmetric key” encryption and “public key” encryption often called “asymmetric key” encryption.

The Secret/private key encryption involves the use of a single key to encrypt and to decrypt the content such as controlling access to content in pay-per-view television programme. A scenario that uses secret key to encrypt the program and only customers with valid pay receipt gains access to the secret key in other to activate service reception. Successful application of secret key encryption to protect copyrighted works depends on keeping the key secret as the name suggests – hence, undue exposure of the key will lead to compromising the technology. Symmetric key encryption is essentially useful when encrypting your own information as opposed to when sharing encrypted information. (Steve, 1996)

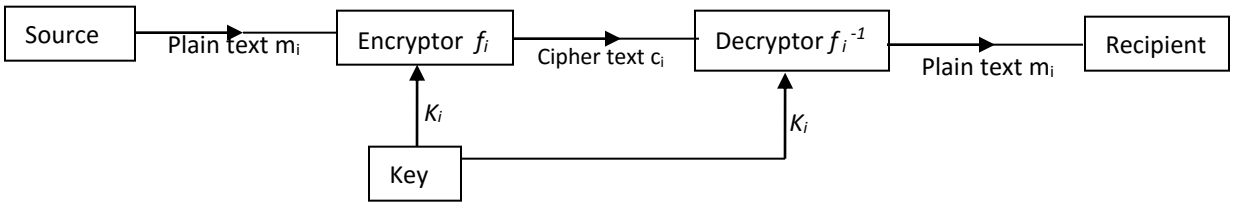

Fig.1: Illustrates using Private Key for Encryption (Kajaraman 2010)

Methodologically, the symmetric key was first implemented as Digital Encryption Standard (DES) and later as Triple Digital Encryption Standard (TDES) by the U.S government in 1977 (Rajaraman,2010).

However, vulnerability was observed with increased speed of computers as code breakers decodes the DES key where sufficiently large amount of input/output data is used. Relatively, Ron Rivest developed the RC2 algorithm in the late 1980s as a replacement for DES. RC2 encrypts data in 64-bit blocks and has a variable key size of 8 to 128 bits in 8-bit increments. Lotus Development requested Rivest's help in creating RC2 for the company's Lotus Notes software. Because a large part of encryption algorithms strength lies in the length of its keys, researchers now consider RC2 to be too easily compromised.

Thus, the introduction of Advanced Encryption Standard AES which breaks up data into 128 bit block and encrypt each block with at least same value. It is very robust and extremely secured in a manner can hardly be broken. AES is used to secure up to 256-bit key length which would take about a billion years for a 10 petaflop computer to guess the key through a brute-force attack.

On the other hand, the Public key (asymmetric) encryption is generally used for distribution of content to a wide audience. It uses an algorithm requiring two keys – a "public" key and a "private" key. The data is encrypted using the public key, which is then made widely available to the public. The private key is kept secret by individuals. The fundamental point is that the encrypted content or secret message can only be decrypted using the corresponding private key.

The scenario here requires that a copyright owner should encrypt a work using the public key of the intended recipient. Once the recipient receives the encrypted transmission, he or she could use the private key to decrypt what is transmitted. No private keys need to be exchanged in this transaction. Without the private key of the intended recipient, the work cannot be read, manipulated or otherwise deciphered easily by casual users.

Implementing an Encryption Algorithm

A prototype encryption algorithm is implemented with these codes outlined thus:

```
$decrypt_code =substr(mt_rand(10000, 10000000), 0, 4);
$cot_code = $_FILES['upload_file']['name'];
#---ENCRYPTION---
  #the key should be random binary, use scrypt, bcrypt or PBKDF2 to
  #convert a string into a key
  #key is specified using hexadecimal
  $key= $decrypt_code;
  #show key size use either 16, 24, or 32byte keys for AES -128, 192,
  #and 256 respectively
  $key_size = strlen($key);
  $plaintext=$cot_code;
  #create a random IV to use with CBC encoding
  $iv_size =mcrypt_get_iv_size(MCRYPT_RIJNDAEL_128, MCRYPT_MODE_CBC);
  $iv=mcrypt_create_iv($iv_size, MCRYPT_RAND);
```

```
#creates a cipher text compatible with AES(Rijndael block size=128)#to keep the text confidential
#only suitable for encodedin put that never ends with value 00h
#(because of default zero padding)
 $ciphertext = mcrypt_encrypt(MCRYPT_RIJNDAEL_128, $key, $plaintext, MCRYPT_MODE_CBC, $iv);
#prepend the IV forittobeavailablefordecryption
$ciphertext = $iv.$ciphertext;
#encodetheresultingciphertextsoitcanberepresentedbyastring
$ciphertext_base64 = base64_encode($ciphertext);
#===WARNING===
#Resultingciphertexthasnointegrityorauthenticityadded
#andisnotprotectedagainstpaddingoracleattacks.
#---DECRYPTION---
$ciphertext_dec = base64_decode($ciphertext_base64);
#retrievestheIV,iv_sizeshouldbecreatedusingmcrypt_get_iv_size()
$iv_dec = substr($ciphertext_dec, 0, $iv_size);
#retrievesthecipher text(everythingexceptthe$iv_sizeinthefront)
$ciphertext_dec=substr($ciphertext_dec, $iv_size);
# may remove 00h valued characters from end of plain text
$plaintext_dec=mcrypt_decrypt(MCRYPT_RIJNDAEL_128,$key, $ciphertext_dec, MCRYPT_MODE_CBC, $iv_dec);
```

DISCUSSION

Digital Resource Access Authentication

Technologies used to identify devices and authenticate the identity of users are important elements of modern technological protection systems. Foremost among known methods are discussed thus:

1. **IP Authentication:** refers to a measure used to control user access to protected resources in a centralized network through the use of Internet Protocol addresses. To facilitate access to protect content from off-site locations, however, a resource provider may need to provide password accounts to users which also may be stored in a cookie (a text string or small file placed on an end user's piece).

2. **Digital Certificates**; by this approach, the identity of users is authenticated by a certificate authority (CA). This is a body that issues a personal digital certificate containing owner's name, public key & its expiration time, serial number, name of certificate issuer and her digital signature.

3. **Digital Signatures:** is a common cryptographic technique that can be used to authenticate both the contents of a message and the person who signed it. Technologies to authenticate the integrity and source of digital content are also important components of technological protection systems. As it has become easier and easier to tamper with digital works without detection, techniques to

ensure the integrity of digital content have become more important. For example, a publisher of a medical text may depend on content authentication techniques to ensure that textual data (such as dosage amounts) or visual data (such as medical illustration) have not been altered. Digital signatures may be transmitted along with the work as "metadata" (encoded identifying information about the content, discussed more fully below) or embedded directly into the work as watermarks. More broadly, encryption technology may be used to authenticate the integrity of license terms and conditions associated with copyrighted digitized work.

4. **Digital Watermark Process**: Watermarking is a technique for media authentication and forgery prevention and it is viewed as an enabling technology to protect media from reuse without adequate credit or in an unauthorized way (Trowbridge, 1995). Technically, a digital watermark consists of a sequence of numbers, also known as the watermark sequence. The watermark sequence consists of a set of watermark bits. From the signal processing perspective, a digital watermark is a digital signal. Original content (or host signal) is embedded with the digital watermark and it becomes watermarked content or copyright-protected media. Basically, the processes required are watermark insertion, detection and extraction. Moreover, the technical requirements of watermarking techniques also vary from application to application. Swanson, et al. (1998) identified the requirements for the application of copyright protection that watermarking must embed the ownership of the content when the content is being duplicated or abused.

CONCLUSION

Encryption is not an entirely new ideology, but rather new formidable technical advances continue to emerge in other to forestall persistent attempts of social miscreants to trap classical data. In view of this, implementing encryption algorithm for secured digital resource data has proved to be a credible resort. Interestingly, the prototype algorithm displayed above is potentially and proficiently useful in ensuring the security of digital resources such as textual data, audio-visual data, etc. Succinctly, networking and internet operation services engage the popular wireless encryption protocol (WEP) to implement and prevent system invasions.

Appropriate utilization of various authentication mechanisms such as IP authentication, digital certificate, digital signature and digital watermarking greatly abates the rake been meted on digital resources. Therefore, it is instructive to recommend swift adoption and continued engagement of available encryption algorithm – thereby ostensibly create a paradigm driven by evolving technological world.

REFERENCE

Einhora, M. A., and Rosenblatt, B. (2005). Peer-to-Peer Networking and Digital Rights Management: How market tools can solve copyright problems. Carto Institute Policy Analsis no.534

Frattolillo, F., and Landolfi, F. (2008). "Designing a DRM System", in Proceeding of the Fourth International Symposium on Information Assurance and Security, IEEE Computer Society - Los Alamitos, CA. pp221

Hawa, M. (2008). "A Measurement Study of Shared Content on Peer-to-Peer Networks" A Proceedings of the 2008 International Symposium on Performance.

Liebowitz, S. (1985). 'Copying and Indirect Appropriability Photocopying of Journals.' *Journal of Political Economy 93(5) 945–947*. Nathan Associates Study (2006) 'Private Copying Levies on Digital Equipment and Media: Direct Effects on Consumers and Producers and Indirect Effects on Sales of Online Music and Ringtones'.

Rajaraman V. (2010). Introduction to Information Technology. PHI Learning Private Limited, New Delhi. Pp.318-321.

Trowbridge, R (1995). 'Why has Cultural Economics Ignored Copyright?' *The Journal of Cultural Economics 32 243-259*. Towse, R., C. Handke and P. Stepan (2008). 'The Economics of Copyright Law: A Stocktake of the Literature.'

Swanson, J (1998). 'Integrating Consumer Rights into Copyright Law From a European Perspective.' *Journal of Consumer Policy, vol. 31, no. 4*. The Printing Group (2006) 'Statement on Copyright Levies on Multifunctional Printers and Printers.'