BEST: International Journal of Management, Information Technology and Engineering (BEST: IJMITE)
ISSN(Print):2348-0513; ISSN(Online): 2454-471X;
Vol. 3, Issue 9, Sep 2015, 95-100
© BEST Journals

INTRODUCING A NEW CRYPTOGRAPHIC SCHEME: AK CIPHER

ABHISHEK DADHWAL & KOMAL RAJPAL

Master of Computer Applications (MCA), Guru Gobind Singh Indraprastha university (GGSIPU), Delhi, India

ABSTRACT

Disclosure of information or leakage of data in an untrusted environment may lead to unauthenticated access to the confidential information and systems security. Whenever a message is transmitted by a sender to a receiver, it means to have a complete protection from ground to up so that no attacker may gain any access to private information. The information exchange, now a days, underlie most modern security protocols. Many schemes have been applied since the security has been considered as the key agreement. [1]For instance-sending sensitive information like social security, passport or credit card numbers, via email is necessary, at such points encrypted message sending is considered. A key is, therefore, provided for encryption process of the sender's message and encrypted message is then decrypted at the receiver's side. In this way a secure message is transferred. Formalisation of a proposed technique, AK Cipher, combines two strong techniques and guarantees two times safer sending and receiving which has been shown practically.

Different security channels and tools have been provided to prevent unauthorized access for the exchange of data between two parties. Thus, granting information secrecy and authenticated access. Nevertheless, proposed technique improves encryption security.

KEYWORDS: Integrity, Security.

Encryption: Encoding a plain text to convert it into cipher text.

Decryption: Decoding a cipher text to obtain the original message.

Authentication: Sender's message must be received by right receiver.

Integrity: No modifications or alterations with the data must be done.

[3]Plaintext: The intelligible message which will be converted into an unintelligible (encrypted) message.

[3]Ciphertext: A message in encrypted form.

[3]Key: A parameter used in the encryption and decryption process.

[3]Cryptosystem: A system to encrypt and decrypt information