Calculus Cryptography

Mathematics

KEYWORDS : Calculus cryptography, wireless link, encryption, industrial package.

CRS BHARDWAJ

33, first floor, BDA layout, HAL IInd stage, Kodihalli, 6th main, Bangalore

ABSTRACT

This analysis paper discusses the 'Calculus Cryptography' that's that the art of fixing the message into cipher kind. ASCII code, decimal number, octal number and hexadecimal numbers square measure unit are reborn into polynomial kind. This polynomial equation is differentiated or integrated. The polynomial coefficients and degrees square measure unit combined to form the amount before transmission. As we tend to all recognize that there is variety of package accessible among the market that's utilized for the cryptography and secret writing. Some agencies have automatic secret writing sets. These sets square measure used for the investigation to decipher the message. Among calculus cryptography the important message is encrypted by calculus beforehand. Throughout the transmission alone calculus unit transmitted with the operation of the key. The bilaterally symmetrical secret is used by the terminals. The inflicting of the message is safe on line than the wireless set.

Introduction:

The secrecy of the communications plays a vital role within the business and armed forces transactions. The progress of someone or a corporation depends on the security and security of on-line knowledge communications. In modern world, for businesses and within the military wars there's an important and significant role of cyber security. The counsel is passed on the net for the industrial functions. The counsel system is that the key of success throughout the wars and trades. Numerous Symmetric-keys and asymmetric-keys sort security protocols are developed to induce eliminate the issues. Till you've got one thing secret in your hand, it is leaked anyplace within the middle throughout the transmission. Infinitesimal calculus Cryptography has been explained that relies on the on top of reality. The industrial cryptography / secret writing package are used throughout the transmission once infinitesimal calculus cryptography.

Symmetric-key encryption techniques Symmetric-key algorithms[1] are a class of algorithms for cryptography that use the same cryptographic keys for both encryption of plaintext and decryption of ciphertext. The keys may be identical or there may be a simple transformation to go between the two keys. Examples of popular and well-respected symmetric algorithms include Twofish, Serpent, AES (Rijndael), Blowfish, CAST5, RC4, 3DES, and IDEA.

Asymmetric key encryption techniques

There are two related keys--a key pair. A public key is made freely available to anyone who might want to send you a message. A second, private key is kept secret, so that only you know it. Any message (text, binary files, or documents) that are encrypted by using the public key can only be decrypted by applying the same algorithm, but by using the matching private key. Any message that is encrypted by using the private key can only be decrypted by using the matching public key. Various asymmetric encryption algorithms (RSA, Elgamal) have been implemented [5].

Pretty good privacy (pgp) is a data encryption and decryption computer program that provides cryptographic privacy and authentication for data communication. PGP is often used for signing, encrypting and decrypting texts, e-mails, files, directories and whole disk partitions to increase the security of e-mail communications. Current versions of PGP encryption include both options through an automated key management server [6].

Materials, apparatus and procedures

The procedures of encryptions that square measure explained higher than aren't thus reliable as a result of they will even be decrypted by victimization an equivalent software package. The complete spy uses all sorts of business software package to extract the knowledge. Any secret writing methodology isn't secure as a result of it's additionally decryption software package. Once it's derived, your data is decoded by your enemy. Until the knowledge isn't in your hand it is leaked out actually. If you're the primary and last man to decipher the knowledge then sourly you'll get through. Before transmission of the message it ought to be encrypted domestically by victimization the native techniques. Some strategies of calculus cryptography square measure given below.

Method 1:- The calculus can be used to encrypt the message. If the serial number of the alphabet is from one to twenty six then A can be written as x1 and the letter Z can be written as x26.

$y = x^{1,}$ (letter A)

$\frac{dy}{dx} = 1\, x^{\circ},$ The code for the letter A is 10

$y = x^2$

$\frac{dy}{dx} = 2\, x^{1},$ The code for the letter B is 21

$y = x^3$

$\frac{dy}{dx} = 3\, x^{2},$ The code for the letter C is 32

$y = x^4$

$\frac{dy}{dx} = 4\, x^{3},$ The code for the letter D is 43

………………………………………………

……………………………………………………

$y = x^{26}$

$\frac{dy}{dx} = 26\, x^{25},$ The code for the letter Z is 2625

At the receiving end the equation can be integrated to get the original number.

$I = \int 26\, x^{25} dx = x^{26}$

After calculus cryptography the message can be transmitted by using any crypto software.

Method 2:-
The ASCII code of the alphabet are from 1000001 to 1011010 (A to Z). These codes can be written in the polynomial form. The polynomial form for the letter A (1000001) is $x^7 + x^1$. The polynomial form for the letter Z (1011010) is $x_7 + x^5 + x^4 + x^2$

$y = x^7 + x^1$

$\frac{dy}{dx} = 7x^6 + 1.x^0$, The code for the letter A in the ASCII form is 7610.

$y = x^7 + x^5 + x^4 + x^2$

$\frac{dy}{dx} = 7x^6 + 5.x^4 + 4x^3 + 2.x^1$,

The code for the letter Z in the ASCII form is 76544321

At the receiving end the equation can be integrated to get the original number.

$I = \int(7x^6 + 1.x^0)dx = x^7 + x^1$,

Code for the letter A can be generated as 1000001.

$I = \int(7x^6 + 5.x^4 + 4x^3 + 2.x^1)dx =$

$x^7 + x^5 + x^4 + x^2$, Code for the letter Z can be generated as 1011010.

Method 3:- The octal code of the alphabet are from 101 to 132 (A to Z). These codes can be written in the polynomial form. The polynomial form for the letter A (101) is $x^3 + x^1$. The polynomial form for the letter Z (132) is $x^{31} + x^{23} + x^{12}$

$y = x^3 + x^1$

$\frac{dy}{dx} = 3x^2 + 1.x^0$,

The code for the letter A in the octal form is 3210.

$y = x^{31} + x^{23} + x^{12}$

$\frac{dy}{dx} = 31x^{30} + 23.x^{22} + 12x^{11}$,

The code for the letter Z in the octal form is 313023221211

At the receiving end the equation can be integrated to get the original number.

$I = \int(3x^2 + 1.x^0)dx = x^3 + x^1$,

Code for the letter A can be generated as 101.

$I = \int(31x^{30} + 23.x^{22} + 12x^{11})dx =$

$x^{31} + x^{23} + x^{12}$, Code for the letter Z can be generated as 132.

Method 4:- The decimal code of the alphabet are from 65 to 90 (A to Z). These codes can be written in the polynomial form. The polynomial form for the letter A (65) is x6 + x5. The polynomial form for the letter Z (90) is x9+ x0

$y = x^6 + x^5$

$\frac{dy}{dx} = 6x^5 + 5.x^4$,

The code for the letter A in the decimal form is 6554.

$y = x^9 + x^0$

$\frac{dy}{dx} = 9x^8 + 0.x^{-1}$,

The code for the letter Z in the decimal form is 980

At the receiving end the equation can be integrated to get the original number.

$I = \int(6x^5 + 5.x^4)dx = x^6 + x^5$, Code for the letter A can be generated as 65.

$I = \int(9x^8 + 0.x^{-1})dx = x^9 + x^0$, Code for the letter Z can be generated as 90.

Method 5:-The Hexadecimal code of the alphabet is from 41 to 5 A (A to Z). These codes can be written in the polynomial form. The polynomial form for the letter A (41) is x4 + x1. The polynomial form for the letter Z (90) is x5+ xA

$y = x^4 + x^1$

$\frac{dy}{dx} = 4x^3 + 1.x^0$,

The code for the letter Z in the Hexadecimal form is 4310.

$y = x^5 + x^A$

$\frac{dy}{dx} = 5x^4 + 10.x^9$,

The code for the letter Z in the Hexadecimal form is 54109.

At the receiving end the equation can be integrated to get the original number.

$I = \int(4x^3 + 1.x^0)dx = x^4 + x^1$, Code for the letter A can be generated in hexadecimal form as 41.

$I = \int(5x^4 + 10.x^9)dx = 5x^4 + 10.x^9$, Code for the letter Z can be generated as 5 A.

Implementation:- The implementation suggests that to put in the software package. By using the calculus cryptography the software package can be prepared in advance. These technologies also can cook pan within the adverse condition once the business links square measure within the sender scan or receiving system scan.

Discussion:-The calculus cryptography is superior to the other cryptography techniques because it involves differentiations and integrations which are unapproachable for nonmathematical persons. The symmetrical secret writing is used as a result of it's quite quicker than uneven secret writing.

The calculus cryptography also can be accustomed pass the message on phone or lines and on the radio nets. Mobiles services also can be used throughout the war as a result of the actions square measure taken terribly quickly at intervals one hour.

The calculus Cryptography is a fancy method as a result of the message remains within the cipher type. The right person is needed to decipher the message.

The parties at the terminal finishes should be able to use calculus Cryptography. It's not possible to use calculus Cryptography unless individuals at each end square measure capable of victimization this.

Conclusion: - This analysis paper discusses the 'Calculus Cryptography' that's that the art of fixing the message into cipher sort. ASCII code, decimal number, octal number and hexadecimal numbers are unit reborn into polynomial sort. This polynomial equation is differentiated or integrated. The polynomial coefficients and degrees are unit combined to make the number before transmission. By the application of the key the message can be made more critical.

REFERENCE

| 1. Delfs, Hans & Knebl, Helmut (2007)."Symmetric-key encryption". | 2. Belfield, R. (2007). The Six Unsolved Ciphers: | 3. Diffie, W., & Landau, S. (1998). Privacy on the Line. Boston: MIT Press. | 4. Electronic Frontier Foundation. (1998). | 5. Federal Information Processing Standards (FIPS) 140-2. (2001, May 25). |