Geo-Encryption Algorithm

1. Abstract

1.1 Cryptography - confidentiality, data integrity, entity authentication and data origin authentication

1.2 Feistel Cipher

1.3 Little about the algo – (Symmetric and Block cipher)

2. Introduction

1.1 Symmetric/Asymmetric Algorithms

The fundamental difference that distinguishes symmetric and asymmetric encryption is that symmetric encryption allows encryption and decryption of the message with the same key. Whereas, asymmetric encryption uses the public key for the encryption, and a private key is used for decryption.

1.2 Block and Stream Cipher

In Block cipher, Algorithms take a large block of the text to be encode, typically 64 to 128 bits and encode it using a Key. This same key is used to encode the other parts of the text.

In Stream Cipher, Algorithms take a relatively small blocks of one bit or one byte long and encode them with a Key and many previous blocks. The algorithm uses different key for each bit/byte encoding.

1.3 Areas of Application

Encrypting Data Files or Data Streams

Random Bit generator

Packet Encryption – ATM PIN, Messaging

1.4 Platforms

Microprocessors

Large Hardware Systems

1.5 Additional Requirements

1.6 Design Decisions

No weak keys as a design goal

3. Literature Survey:

1.1 Elliptic curve cryptography

[https://andrea.corbellini.name/2015/05/17/elliptic-curve](https://andrea.corbellini.name/2015/05/17/elliptic-curve-)-cryptography-a-gentle-introduction/

1.2 AES

1.3 3DES

1.4 Blowfish

4. Building Blocks

5. Description of the Algorithm

6. Possible Simplifications/ Decisions

7. Conclusions

8. References

====================

Performance Measure

Benchmarking – Handling Attack types

How is the Algorithm resistant to brute force attack?

A brute force attack tries all the possible keys and looks for the one which gives the decrypted data. The length of the key determines the number of possible keys and hence the feasibility of the attack. Algorithms like AES increase the size of the key to escape these types of attacks. In Geo-Encryption algorithm the keys are based on the sectors which are being selected up randomly and therefore it is not certain that the characters will have the same key. Even if the same characters are encrypted again and again, they would be selecting a random key based on the sectors each time.

https://www.eetimes.com/document.asp?doc\_id=1279619#

Comparison with other Algorithms