A SYSTEM FOR GENERATING STREAM-CIPHERED DOUBLE-KEY USING A RANDOMIZED-MATRIX FOR VARIED LENGTH TEXT AND IMAGE

Technology Description

The work presents a system for generating stream-ciphered double-key using a randomized matrix for varied-length text and image encryption and decryption. The encryption is done with multiple layers of randomization and 2 keys are generated in order to enhance the security of the data. By using this encryption algorithm, the resultant encrypted data is claimed to provide security even against quantum computers because the security of the system is measured with n factorial contrary in terms of 2^n. It also has secondary security that is obtained when the second key is generated.

There are various cryptographic systems that were and are very secure, but as quantum computers are going to be a new reality in the coming decade, the security of the existing cryptographic systems will be compromised. The new ongoing practice in the hacker community is known as "Harvest Now – Decrypt Later" where encrypted data is collected now to be decrypted in the future with the help of quantum computers.

This invention aims to provide the following primary properties during the encryption process:

One-time padding; Easy customizability; Double-key generation; Multiple layer of randomization

There are various encryption techniques that implement the block cipher technique where the plain text is converted into cipher text using a fixed-size data block at a time using a shared, secret key. Whereas the stream cipher approach is assumed to be relatively complex and uses one byte of plain text at a time.

The system can provide secure communication while protecting classified information like Industrial and medical research as well as confidential government intelligence data. Also, it can provide to protect conventional transaction data like account numbers and transaction amounts.

Technology Components

Key components involved include:

- ➔ **Cryptography (Stream Cipher)**: For secure text and image encryption.
- ➔ **Quantum-Resistant Encryption**: Designed to withstand decryption attempts by quantum computers.
- ➔ **Randomization and Key Generation**: Uses randomized matrices and double keys to improve security.

Applications

- **Secure Communication**: Protects sensitive communications, such as government intelligence, military data, and classified corporate information.
- **Financial Transactions**: Ensures the security of banking and payment systems by encrypting transaction data like account numbers and payment details.
- **Industrial and Medical Research**: Safeguards confidential research data in industries like pharmaceuticals, biotechnology, and advanced manufacturing.
- **Government Data Protection**: Secures confidential government documents and classified communications from future quantum attacks.
- **Healthcare Data**: Protects sensitive patient data and medical records from unauthorized access.
- **Cloud Data Security**: Provides encryption for data stored in cloud environments, protecting against potential future decryption by quantum computers.

Who can be the potential users?

- **Government Agencies**:
  Departments handling classified information and sensitive national security data.
- **Military Organizations**:
  Armed forces needing to secure communications and protect strategic information.
- **Healthcare Institutions**:
  Hospitals and medical research facilities requiring protection for patient data and medical research.
- **Financial Institutions**:
  Banks and financial service providers that need to secure transaction data and account information.
- **Corporate Enterprises**:
  Companies involved in research and development that require encryption for proprietary information and intellectual property.
- **Telecommunications Providers**:
  Businesses offering secure communication services to clients, particularly in industries that require high levels of confidentiality.
- **Cybersecurity Firms**:
  Companies specializing in protecting digital assets, data privacy, and providing encryption solutions.

List of Features:

- **Quantum-Resistant Encryption**: Provides enhanced security that is resistant to attacks from quantum computers.
- **Double-Key Generation**: Uses two keys for encryption, adding an extra layer of security.
- **Multiple Layers of Randomization**: Ensures that the encryption is highly randomized, making it difficult for attackers to predict.
- **Stream Cipher Approach**: Encrypts data one byte at a time, allowing for efficient and flexible encryption of varying-length data.
- **One-Time Padding**: Implements a one-time pad encryption method for an extra level of security.
- **Customizability**: Easily customizable to fit specific security needs or data types.
- **Protection Against "Harvest Now – Decrypt Later" Threats**: Prevents encrypted data from being decrypted in the future by quantum computers.

THEME : Cybersecurity and Cryptography

DOMAINS :

- Finance and Banking
- Healthcare
- Government and Defense
- Telecommunications
- E-Commerce
- Education
- Legal Services
- Energy and Utilities

- **Tech ID : I005**
- **Patent : Filed**
- **Owner :** Dr. Meenakshi Malhotra
- **Contact Us : alok@iiitd.ac.in**