Encryption & Decryption Algorithms

CS 218 : Data Structures and Algorithms

- By Manan Jain (180010017) & Yuvraj Agrawal (180010031)

Topics Covered by us:

- Problem statement
- Our Solution
- Encryption & Decryption
  - Symmetric Key encryption
  - Asymmetric key encryption
- RSA (Rivest Shamir Adleman) Algorithm
- AES (Advanced Encryption Standards) Algorithm

Our Problem Statement & Solution:

We are trying to model a typical situation in PoK.
The Army outposts regularly want to communicate and exchange sensitive information, but the data is at risk since the adversary might steal our data, interpret it and may use it against us. So we plan to generate a way to secure the communication among the army outposts.

We propose a way through which the army personnel first uses asymmetric encryption (RSA) to request and receive a symmetric AES key for further secure communication. Then the army personnel can record an audio message, convert it to hexadecimal, encrypt this data using symmetric encryption (AES) and deliver it to his allies.

Why combination of AES & RSA

RSA needs two different mathematically linked keys to work. although it does not have the problem of key transport, but it is computationally costly compared to symmetric key algorithms.

Using the combination of AES and RSA, the asymmetric-key algorithm is only used to encrypt the symmetric key, while the data is encrypted with AES. This makes computational cost negligible. And with AES the data is even more secure

So, we get better performance and more secure communication if we use RSA and AES together.

Encryption & Decryption

- **Encryption** is a process that encodes a message or file so that it can only be read by certain people.
- **Decryption** is a way to change encrypted information back into plaintext. This is the decrypted form.
- **Key** : Random string of bits created specifically for scrambling and unscrambling data.
- In **Symmetric encryption** only one key (a secret key) is used to both encrypt and decrypt electronic information. Eg. AES
- In **Asymmetric encryption**, also known as public-key cryptography, a pair of related keys are used, one public key and one private key, to encrypt and decrypt a message respectively. Eg. RSA

RSA (Rivest, Shamir, Adleman)

The algorithm is based on the fact that finding the factors of a large composite number is difficult: when the factors are prime numbers, the problem is called prime factorization. It is also a key pair (public and private key) generator.

The public key consists of two numbers where one number is multiplication of two large prime numbers. And private key is also derived from the same two prime numbers.

The public key (known by everyone) is used to encrypt the message and the private key known just to the key generator is used to decrypt the message.

AES (Advanced Encryption Standard)

The AES encryption algorithm defines numerous transformations that are to be performed on data stored in an array.

The first step of the cipher is to put the data into an array -- after which, the cipher transformations are repeated over multiple encryption rounds.

The first transformation in the AES encryption cipher is substitution of data using a substitution table; the second transformation shifts data rows , and the third mixes columns . The last transformation is performed on each column using a different part of the encryption key(Symmetric key).

Files attached

- Project report (pdf format)
- Codes (Folder containing code in organised format)
    - secure.py (Python code for project)
    - Input (Folder containing input files)
        - input.mp4 (Demo file to execute the encryption & decryption process)
    - Output (Empty folder to store output files)
        - Encrypted hexadecimal message
        - Decrypted hexadecimal message
        - Decrypted message.
    - instructions.txt (Text file containing instructions to use code)

Conclusion:

In this project:

- We introduced the basics of encryption and decryption.
- Then we explained RSA and AES algorithms.
- Then we used these algorithms and model a real life situation of secure data transmission between army personnel.