Encryption Algorithms for Secure Communication over the Internet

BSP S3

BICS winter semester 2018/2019

Summary of report in English

BICS student: Desislava MARINOVA
PATs: PhD Student Asya MITSEVA, Prof. Dr. Thomas ENGEL
Faculty of Science, Technology and Communication
University of Luxembourg

Email:
desislava.marinova.002@student.uni.lu
asya.mitseva@uni.lu
thomas.engel@uni.lu

Nowadays, we depend on online connectivity to carry out various activities among which online banking, accessing medical and governmental records as well as transfer and storage of sensitive information. Hence, it is of vital necessity to protect our data against lurking intruders and potential attacks.

The main domains of this Bachelor semester projects are Cryptography and Network security. In cryptography, the original message is known as *plaintext* or *cleartext*. The process of concealing message's content is *encryption*. Thus, an encrypted message is *ciphertext*. The process of turning ciphertext back into plaintext is *decryption*. A *cipher* is an algorithm for executing a series of steps during encryption or decryption operations. A *cryptosystem* or *cipher system* is an implementation of cryptographic techniques to provide information security services.

There are two types of cryptography: symmetric key and asymmetric key cryptography. For this project, we mainly focus on symmetric-key cryptography, also called conventional. It comprises a single key for both encryption and decryption operations. To use symmetric encryption securely one needs a strong encryption algorithm as well as a secret key known only to sender/receiver. Symmetric-key systems are simpler and faster. However, their main disadvantage is key management, since both parties must exchange the key in a secure way. Otherwise, the key could be intercepted and compromised by a third party leading to decryption of the secret information. To overcome this, asymmetric or public-key cryptography came into existence. It requires two separate keys, one public and one private, for encryption and decryption, respectively. Notwithstanding, many modern ciphers are hybrid cryptographic systems since they use both symmetric-key and asymmetric-key encryption.

The types of operations used in classical symmetric cryptography are substitution and transposition along with two ways in which the plaintext is processed: block and stream.

To begin with, substitution ciphers replace letters of the plaintext with other letters, numbers or symbols. The plaintext is viewed as a sequence of bits where substitution operation replaces plaintext bit patterns with ciphertext bit patterns. The earliest known substitution cipher is Caesar cipher which shifts a letter three positions forward. ROT13 is a special case of Caesar cipher. It encodes the plaintext by13 shifts,

making encryption and decryption identical. Hence, it is its own inverse and is an example of a weak cipher. The One-time pad (OTP) XORs a random sequence of 0's and 1's to plaintext and uses a random key, which is never repeated and is of the same length as the message. Since it completely obscures the original message, it is considered unbreakable. Transposition ciphers rearrange the letter order without altering the actual letters used. Nevertheless, their drawback is that the ciphertext has the same frequency distribution as the plaintext. A representative is the rail fence cipher that writes out message letters diagonally over a number of rows.

Secondly, block ciphers, the most widely used cryptographic algorithms for encrypting communication over the Internet, process messages into entire blocks at a time, each of which is then encrypted or decrypted. Block ciphers work similarly as substation ciphers but on 64-bit (e.g., DES) or more characters (e.g., AES' 128-bit block length). Stream ciphers, on the other hand, process messages a bit or byte at a time, individually, when encrypting or decrypting. However, sometimes they require fewer resources for implementation than block ciphers which makes them suitable for constrained environments (e.g., cell phones).

Data Encryption Standard (DES) is a modern block cipher, standardized in 1979. It has a 64-bit key comprised of 8-bit parity, leaving a length of 56-bits for the key itself. DES has a 64-bit input and produces a 64-bit output. The 56-bit key generates keys throughout the sixteen 48-bits rounds. The process of permutation is used twice during the algorithm: once before the sixteen rounds and one final time before the 64-bit output. DES, along with other block ciphers, supports several modes of operations: Electronic Cook Book (ECB), Cipher Block Chaining (CBC), Output Feedback (OFB), Cipher Feedback (CFB), Counter mode (CTR) which are used when we want to encrypt larger than 16-bytes plaintext. Nevertheless, DES is nowadays considered insecure. It has been replaced by Triple DES (3DES) which encrypts data three times in contrast to DES. In particular, the one 56-bit key becomes three individual keys, rendering a 168-bit key. Nowadays, one of the most widely used ciphers, due to its security, is the Advanced Encryption Standard. AES comprises three block ciphers: AES-128, AES-192 and AES-256. Each cipher has a 128-bit block length, with key sizes of 128, 192 and 256 bits, respectively.

We build a Python chat application that encrypts user's messages before transmitting them over the Internet. Basic programming skills in Python are needed along with clear comprehension of basic cryptographic primitives. The encryption algorithms reviewed in our project are Caesar cipher, ROT13, One-time pad (OTP), Vigenere cipher, Enigma machine, Rivest cipher 4 (RC4), DES, 3DES, and AES. Our chat application makes use of Caesar cipher, ROT13, DES and AES. The latter two have been implemented using the support of PyCryptodome library. Our chat application relies on a client/server architecture. We have chosen TCP networking as a communication endpoint. Once the server and client establish a connection, the client can send encrypted messages to the server using the four algorithms listed above. The server decrypts the ciphertext and echoes the plaintext back to the client. We measured the time it took for each algorithm to execute the operations of encryption and decryption. We experimented with a message of size 100 bytes. An overall observation to be made is that Caesar cipher and ROT13 produced identical results.
DES outperformed AES as it is using less resources. Furthermore, DES's mode of operation ECB is simple and does not require an initialization vector (IV). AES's mode of operation CBC is more secure

and complex than ECB, hence it took more processing time for AES to produce encryption and decryption outputs.

In fine, we presented a secure communication over the Internet by implementing symmetric-key encryption algorithms. Nowadays, it is imperative to establish encrypted and authenticated flow of confidential information over insecure channels. At a continually increasing rate, we observe that public institutions and private organizations are turning to cryptography and cryptosystems in order to identify and overcome cyber risks and threats. This is a major step toward a smart environment where businesses, information, and social processes communicate and interact with each other to secure the Internet traffic of the future.

1063 words