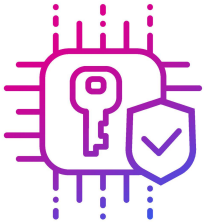
Breaking DES

Danyelle Palmore, Kaciopey Ikounga, Drew Walker

Table of contents

01

Importance of Breaking DES



Why is it important

Data encryption is important because it prevents unauthorized access to your data and helps protect sensitive information. Decryption is used to make sense of encrypted data. It could be used for either good or bad reasons

Why is it useful

Good ways people use it

- **Law enforcement investigation**: Data may need to be decrypted during a criminal investigation.
- **Data recovery**: Help recover lost data
- **Security Audits**: Used to identify vulnerabilities. Decrypting data helps assess the effectiveness of the encryption method
- **Research and development**: Encryption algorithms are studied to improve security or develop new encryption techniques

Harmful ways

- **Espionage**: cybercriminals might break encryption to gain access to sensitive information, trade secrets.
- **Financial gain**: Cybercriminals may target encrypted financial transactions, steal credit card details, or access bank accounts.
- **Privacy invasion**: might break encryption to invade someone's privacy, such as accessing personal emails or private messages
- **Ransomware**: Decrypting data encrypted by ransomware is essential for victims who want to regain access to their files.
- **Cyberwarfare**: Nation-states may break encryption during cyberwarfare to disrupt communication or gain an advantage.

02
Problem Definition

Introduction

Breaking Data Encryption Services involves identifying vulnerabilities in data encryption mechanisms to access or manipulate encrypted information without authorization. This can encompass various tactics, such as exploiting weaknesses in encryption algorithms, gaining unauthorized access to encryption keys, or finding flaws in the encryption implementation. Successful breaches can lead to severe consequences, including data theft, unauthorized data modification, and privacy violations. Addressing this problem requires robust encryption standards, secure key management, and regular security audits to identify and remediate vulnerabilities.

About This Problem

Attack Methods:

- Exploiting flaws in encryption algorithms.
- obtaining illegal access to encryption keys.
- Detecting implementation problems or security loopholes

Protecting encryption services is critical for data security. Vigilance and proactive security measures are essential to prevent unauthorized access to encrypted information.

Potential consequences include Data theft or leakage, unauthorized data modification, violating privacy and security regulations

Mitigation Strategies:

Use strong encryption methods and protocols.

Implement secure key management techniques.

Perform regular security audits and penetration testing to identify weaknesses.

03
Solutions & Demo

Go over the proposed solutions and demo our code

Demo of DES

Online Cryptography Tools

DES Algorithm Proposals

Project	Time	Algorithm
DESCHALL Project 1997	7 billion keys per second	Many people searching key space through brute force
EFF DES Cracker “Deep Crack” (56 hours) 1998	90 billion keys per second	Single PC assigned ranges of keys to the chips

DES Brute Force Algorithm

Decrypt an encrypted message trying every possible key.

Generate Key

56 bit DES key generated using key generation algorithm

Encrypt

Plaintext data is divided into blocks of 64 bits. Each block is encrypted using the DES algorithm and the generated key

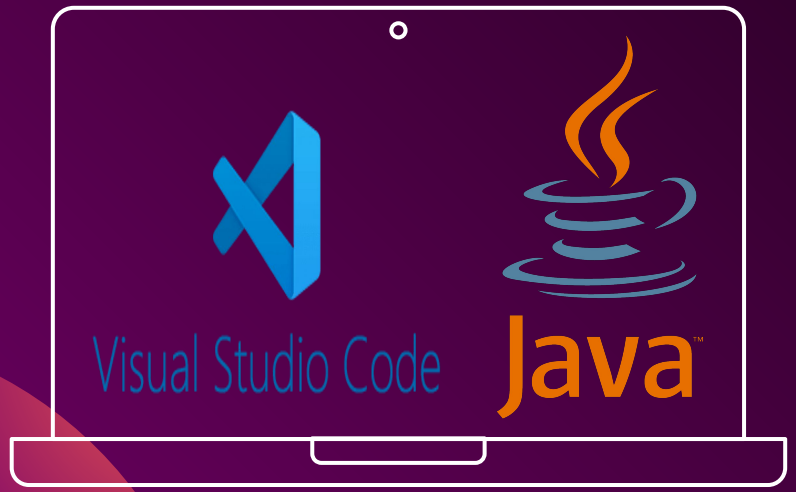
Decrypt

The encrypted data can be decrypted using the same key and the decryption algorithm. The decryption process is similar to encryption but in reverse, with the order of keys reversed.

The Code

```java
//Java classes that are mandatory to import for encryption and decryption process
import java.io.FileInputStream;
import java.io.FileOutputStream;
import java.io.IOException;
import java.io.InputStream;
import java.io.OutputStream;
import java.security.InvalidAlgorithmParameterException;
import java.security.InvalidKeyException;
import java.security.NoSuchAlgorithmException;
import java.security.spec.AlgorithmParameterSpec;
import javax.crypto.Cipher;
import javax.crypto.CipherInputStream;
import javax.crypto.CipherOutputStream;
import javax.crypto.KeyGenerator;
import javax.crypto.NoSuchPaddingException;
import javax.crypto.SecretKey;
import javax.crypto.spec.IvParameterSpec;
public class DesProgram
{
//creating an instance of the Cipher class for encryption
private static Cipher encrypt;
//creating an instance of the Cipher class for decryption
private static Cipher decrypt;
//initializing vector
private static final byte[] initialization_vector = { 22, 33, 11, 44, 55, 99, 66, 77 };
//main() method
Run | Debug
public static void main(String[] args)
{
//path of the file that we want to encrypt
String textFile = "c:/Users/danye/Desktop/DemoData.txt";
//path of the encrypted file that we get as output
String encryptedData = "c:/Users/danye/Desktop/encrypteddata.txt";
//path of the decrypted file that we get as output
String decryptedData = "c:/Users/danye/Desktop/decrypteddata.txt";
try
{
//generating keys by using the KeyGenerator class
SecretKey scrtkey = KeyGenerator.getInstance("DES").generateKey();
AlgorithmParameterSpec aps = new IvParameterSpec(initialization_vector);
//setting encryption mode
encrypt = Cipher.getInstance("DES/CBC/PKCS5Padding");
encrypt.init(Cipher.ENCRYPT_MODE, scrtkey, aps);
//setting decryption mode
decrypt = Cipher.getInstance("DES/CBC/PKCS5Padding");
decrypt.init(Cipher.DECRYPT_MODE, scrtkey, aps);
//calling encrypt() method to encrypt the file
encryption(new FileInputStream(textFile), new FileOutputStream(encryptedData));
//calling decrypt() method to decrypt the file
decryption(new FileInputStream(encryptedData), new FileOutputStream(decryptedData));
//prints the stetment if the program runs successfully
System.out.println(x:"The encrypted and decrypted files have been created successfully.");
}
//catching multiple exceptions by using the | (or) operator in a single catch block
catch (NoSuchAlgorithmException | NoSuchPaddingException | InvalidKeyException | InvalidAlgorithmParameterException | IOException e)
{
//prints the message (if any) related to exceptions
e.printStackTrace();
}
}
//method for encryption
private static void encryption(InputStream input, OutputStream output)
throws IOException
{
output = new CipherOutputStream(output, encrypt);
//calling the writeBytes() method to write the encrypted bytes to the file
writeBytes(input, output);
}
//method for decryption
private static void decryption(InputStream input, OutputStream output)
throws IOException
{
input = new CipherInputStream(input, decrypt);
//calling the writeBytes() method to write the decrypted bytes to the file
writeBytes(input, output);
}
//method for writting bytes to the files
private static void writeBytes(InputStream input, OutputStream output)
throws IOException
{
byte[] writeBuffer = new byte[512];
int readBytes = 0;
while ((readBytes = input.read(writeBuffer)) >= 0)
{
output.write(writeBuffer, off:0, readBytes);
}
//closing the output stream
output.close();
//closing the input stream
input.close();
}
}
```

Product demo



Switch to VSCode

04

Understanding and Improvements

Our Understanding

Encryption

Mathematical procedures used to transform plaintext into ciphertext, ensuring data confidentiality and security by making it accessible only to authorized parties.

Key Generation

Process of creating unique cryptographic keys used for encryption, decryption, or other security-related functions in a secure communication system.

Brute Force Algorithms

Problem-solving methods that exhaustively search through all possible solutions or combinations to find a solution, often lacking efficiency but ensuring correctness.

Room For Improvement

Further research:

- S-box Substitutions
- XOR Operations
- Permutations
- Key Schedules

References

“Cryptography Basics: Symmetric Key Encryption Algorithms.” SearchSecurity, www.techtarget.com

“Java Code for DES - Javatpoint.” Www.javatpoint.com, www.javatpoint.com/java-code-for-des.

Kak, Avi. Lecture 3: Block Ciphers and the Data Encryption Standard Lecture Notes on “Computer and Network Security.” 2022.

“What Is Data Encryption Standard?” SearchSecurity, www.techtarget.com

“What Is Decryption? Everything You Need to Know (2023).” Softwarelab.org, softwarelab.org/blog/what-is-decryption/.

Wikipedia Contributors. “Data Encryption Standard.” Wikipedia, Wikimedia Foundation, 4 Aug. 2019, en.wikipedia.org/wiki/Data_Encryption_Standard.