Data Encryption Standard

Supervised by: Rawia Tahrirs Salih

Done by: Abdulrahman Tawffiq

What is DES?

Symmetric encryption algorithm in which the plaintext is put inside a locked box, DES to be applied on it, the plaintext is converted to the encrypted message and it is ready to be sent to the receiver. At the receiver, the Decryption Algorithm will be applied to the encrypted message by using the same secret Key used by the sender (why the same Key ? Because this is symmetric encryption). Note that In symmetric, usually the same algo is used on both sides like DES at sender & receiver.

Elements:

- The message (plain Text)
- Encryption & Decryption Func.
- The secret Key
- The encrypted message (cipher Text)

Notes:

- The plain text, we will change each letter to its hex code then from hex to binary then to be broken into 64-bit blocks.
- The number of alternative keys could be guessed by knowing the Key size. Key size 32 bits, then 2 to power 32 is the number of Alt Keys which will be found within 2.11 mill second.
- Two things to be considered when using any security algo:
    - The nature of the algorithm and how it is complicated
    - The length of the key That's why DES has been broken in 3 days even though the Key size was 56 bits.

The main issue in DES that makes it weaker and less powerful compared with the others is the 56-bit Key size makes it break within 10 hours. Also, the algo itself is weak nowadays.

DES Principles

DES has two main principles which are:

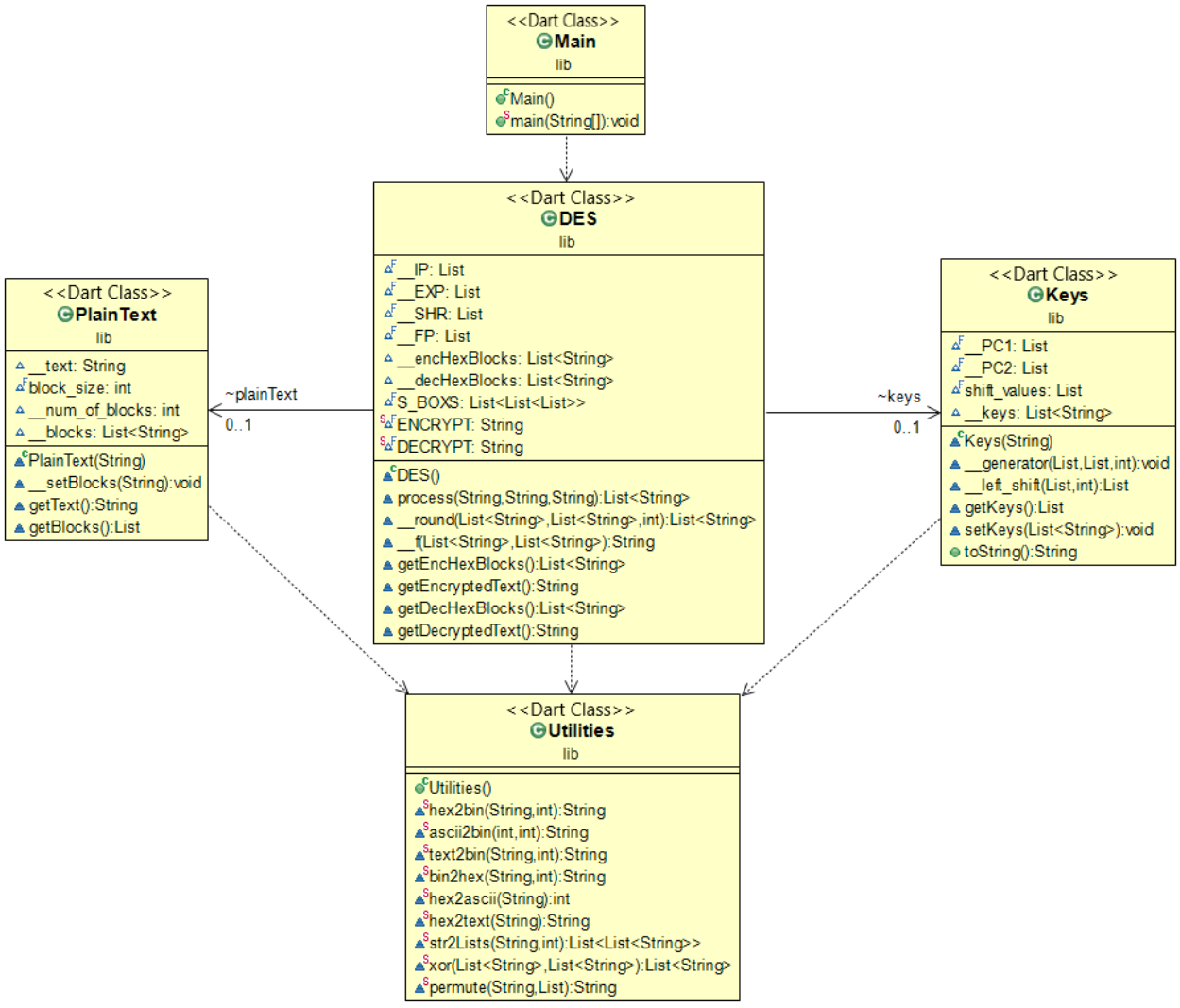
- Diffusion: Each bit in cipher text is dependent on every bit in plaintext to make the relationship between them complicated)
- Confusion: Makes the relationship between the cipher text and the key be as complex as possible)

Those two principles could be done by using substitution and permutation techniques.

1. Substitution: The process of replacing a letter or a bit with another letter or another bit. Example: “car ”will be “snw”.
2. Permutation: The process of only changing the positions of letters or bits

Coding DES Using Dart Programming Language

UML Diagram



Results

lib > Main.dart > ...

```dart
import 'DES.dart';

Run | Debug
void main(List<String> args) {
  String message = "It is secure";
  String key = "AABB09182736CCDD";

  DES des = new DES();
  des.process(message, key, DES.ENCRYPT);
  print("The message: '${message}' has been encrypted to => ${des.getEncryptedText()}");

  des.process(des.getEncryptedText(), key, DES.DECRYPT);
  print("The message: '${des.getEncryptedText()}' has been decrypted to => ${des.getDecryptedText()}");

}

```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL

```
The message: 'It is secure' has been encrypted to => 4hØZ`~ãôB[
The message: '4hØZ`~ãôB[' has been decrypted to => It is secure
Exited
```