🧐

SRP - LAB 3

Symmetric key cryptography

Cilj vježbe: enkriptirati zadani tekst dekriptiran 22-bitnim ključem koristeći brute-force attack (ključ nam je nepoznat)

Plaintext dekriptiran je Fernetom.

Fernet koristi sljedeće *low-level* kriptografske mehanizme:

- AES šifru sa 128 bitnim ključem u CBC enkripcijskom načinu rada
- HMAC (*hash MAC*) sa 256 bitnim ključem za zaštitu integriteta poruka
- Timestamp za osiguravanje svježine (*freshness*) poruka

Ključ kojim je tekst zadan u zadatku enkriptiran za prvih 106 bitova imao je nulu, a preostala 22 bila su nasumično generirana, tj imamo 2^22 mogućih ključeva.

Brute-force napad izvodimo tako da zadani cipertext dekriptiramo sa svakim od mogućih ključeva i provjeravamo jesmo li dobili “nešto smisleno”.

Ono što je enkriptirano zapravo je .png slika, tako da naše “nešto smisleno” bit će predefiniranih 8 bitova koji svaki .png file sadrži na početku:

The first eight bytes of a PNG file always contain the following (decimal) values:

```
137 80 78 71 13 10 26 10
```

Nakon svake dekripcije, uspoređujemo je li prvih 8 bajtova dobivenog plaintexta jednako bajtovima koji se nalaze na početku svakog .png filea.

Ako jesu, uspješno smo pronašli ključ.

pseudokod brute-force attacka

```
for(test_key = 0; test_key < 2^22; test_key++){
    if(decrypt (cipertext with test_key) == “137 80 78 71 13 10 26 10”)
        print (”The key is %test_key”);
        break;
}
```

Rezultat je bio .png file s našim imenom i prezimenom.