Efeito Avalanche

A ideia do efeito avalanche é mensurar a taxa de bits diferentes entre os textos cifrados e claro.

a. Criando mensagens

Utilizando o comando abaixo, foi gerada uma mensagem aleatória M1.

```
openssl rand --hex 16 | head --bytes=16 > M1
```

A mensagem contém 16 bytes e o seguinte conteúdo: `3e8628940d67fcd2`.

b. Criando chave

A seguir, criamos uma chave de 128 bits e salvamos como hexadecimal. Chave K: `bef08db60f5411fc4da16655171ae133`.

```
openssl rand --hex 16 > K
```

c. Duplicando mensagens

Iremos agora duplicar as chaves M1 e alterar manualmente um único bytes da mensagem. A nova mensagen será salva como M1'.

Em nosso exemplo, o último byte foi alterado de `d2` para `d3`.

M1	M1'
3e8628940d67fcd2	3e8628940d67fcd3

Alguns editores de textos irão inserir um caracter de nova linha no final do arquivo, por isso devemos remover esse útlimo caracter para garantir os 16 bytes.

```
cat M1\' | head --bytes=16 > M1\'.tmp
mv M1\'.tmp M1\'
```

d. Cifrando a mensagem

Agora, iremos cifrar a mensagem M1 através do seguinte comando:

```
CYPHER_KEY=$(cat K)
cat M1 | openssl enc -aes-128-ecb -K ${CYPHER_KEY} -nopad > C1

xxd C1
00000000: 5d4f 6324 2ff6 25e2 82e6 15f1 3f33 8126  ]Oc$/.%.....?3.&
```

e. Cifrando a mensagem alterada

Vamos fazer o mesmo para a mensagem alterada.

```
CYPHER_KEY=$(cat K)
cat M1\' | openssl enc -aes-128-ecb -K ${CYPHER_KEY} -nopad > C1\'

xxd C1\'
00000000: 137d 01b7 614a 561f d0f5 7903 448a 93bb  .}..aJV...y.D...
```

f. Comparando os resultados

Através de um programa auxiliar encrito em python `calc-bits.py` nós podemos calcular a taxa de bits diferentes.

```
BITS_C1=$(xxd -b C1 | cut -d ' ' -f 2-7 | tr -d ' ' | tr -d '\n')
BITS_C1L=$(xxd -b C1\' | cut -d ' ' -f 2-7 | tr -d ' ' | tr -d '\n')
./calc-bits.py "$BIT_C1" "$BIT_C1L"
0.53125
```

Resultado: $\sim= 53\%$ de diferença.

g. Automatizando o processo

Para comodidade, podemos executar o exercício de forma automatizada usando o script `generate.sh`.

Para gerar as mensagens, use o seguinte comando:

```
./generate.sh
Preparando diretório data...
~/github/gvicentin/inf0500/inf0570/1-avalanche/data ~/github/gvicentin/inf0500/inf0570/1-ava
Gerando mensagens...
Gerando chave...
----------------------------------------------------------------------
Edite manualmente 1 byte nas mensagens M1', M2'... M10'.
Os arquivos M1', M2'... M10' foram editados? (Enter para continuar)
Cifrando mensagens...
Calculando taxa de bits diferentes...
Mensagem: M1, taxa de bits diferentes: 0.53125
Mensagem: M2, taxa de bits diferentes: 0.578125
Mensagem: M3, taxa de bits diferentes: 0.453125
Mensagem: M4, taxa de bits diferentes: 0.5546875
Mensagem: M5, taxa de bits diferentes: 0.484375
Mensagem: M6, taxa de bits diferentes: 0.5
Mensagem: M7, taxa de bits diferentes: 0.4921875
Mensagem: M8, taxa de bits diferentes: 0.5234375
Mensagem: M9, taxa de bits diferentes: 0.46875
Mensagem: M10, taxa de bits diferentes: 0.4921875
```

h. Alterando a chave

Alterando apenas o último bytes da chave, de `33` para `34` nós obtemos uma diferença de $\sim= 40\%$ neste exemplo. Portanto, o efeito avalanche do AES também se aplica a alterações na chave.