Universidade Federal do Rio Grande do Sul - UFRGS
Disciplina: Segurança em Sistemas de Computação
Prof. Dr. Jéferson Campos Nobre

Atividade Aula 08

Exercício 1

1. Criptografe o texto plano indicado (M=AES is a subset of the Rijndael block cipher developed by two Belgian cryptographers, Vincent Rijmen and Joan Daemen.) usando o template AES Cipher (Text Input) com a chave indicada (K = FD E8 F7 A9 B8 6C 3B FF 07 C0 D3 9D 04 60 5E DD).
2. Produza as análises de frequência considerando o texto claro e o criptografado. Explique.

Exercício 2

1. Quebre o texto criptografado usando o template “AES Analysis using Entropy (1)”.

   25 95 63 95 B6 0A A5 BA 2D 44 61 82 66 E4 32 B5 A4 8D F8 6B 9F 7C 0A B8 C1 0C 33 65 31 18 42 3D 8A 3B C9 DE C3 2C 4D 9B 43 06 78 68 7A F2 95 50 FD F6 97 98 4C C5 03 5D E4 97 BC F2 FB 91 65 AF 52 E5 E2 E3 A6 1B D8 A9 B1 E7 A8 62 52 9A FB DD 6F FE F8 17 97 F8 EC B8 6D FB 19 69 3E B3 CB 70 59 A4 29 05 10 4F 74 E7 D2 7B 57 37 AF A2 7D EE 29 86 0F C3 0F BC 12 8F 1F 93 A4 F1 6F 90 2D 37 AB 04 B6 FD FF 3A F1 62 62 E2 8E 47 1D 70 C5 08 0F 1E 85 21 0D 98 B6 35 54 C3 D3 95 9C 3B 92 DB DC D1 66 0C B7 33 48 70 F3 FC 19 90 A8 BE EC 78 89 67 E1 1C DF 66 5C 06 E8 F1 CD 7C 63 AB 97 BB B0 B0 A1 AD B6 40 4C F1 85 A2 17 21 71 62 5E 53

2. A cifragem utilizada foi AES-128. Um caractere hex corresponde a 4 bit, assim uma chave de 128 bit pode ser descrita por 32 hex chars (32*4=128). Se (K = FF FF FF FF FF FF FF FF FF FF FF FF FF FF ?? ?? ??), quantos bits são desconhecidos?

3. Configure o “Key Searcher” para FF-FF-FF-FF-FF-FF-FF-FF-FF-FF-FF-FF-FF-FF-**-**-**

4. Mesmo ataque anterior, mas com menos bits. Configure o “Key Searcher” para FF-FF-FF-FF-FF-FF-FF-FF-FF-FF-FF-FF-F*-**-**-**

5. Existe diferença no tempo de busca? Explique o porquê.

Referências

- Baseado em material do Prof. Bernhard Esslinger (Universität Siegen)