Criptografia Simétrica

Segurança e Auditoria em Sistemas

Profa. Natássya Barlate Floro da Silva

Universidade Tecnológica Federal do Paraná — Câmpus Cornélio Procópio

16 de Março de 2020

Roteiro

1. DES
2. 3DES
3. *Blowfish*
4. *Twofish*
5. AES

Introdução

- Os principais algoritmos de criptografia simétrica utilizam combinações das técnicas de substituição e transposição.
- Principais algoritmos:
  - DES;
  - 3DES;
  - *Blowfish*;
  - *Twofish*;
  - RC4;
  - AES;

Data Encryption Standard (DES)

- Cifra de bloco;
- Foi um dos algoritmos mais utilizados antes da introdução do AES em 2001.
- Texto claro dividido em blocos de 64 bits.
- Chaves de 56 bits.
- Funcionamento dividido em três fases:
  - Permutação inicial (PI de *Initial Permutation*);
  - 16 rodadas com substituições e permutações;
  - Permutação final (PI^{-1}).
- Hoje é considerado inseguro. Em 2017, foi realizado um ataque de *rainbow table*[1] que permitiu obter a chave do DES em 25 segundos.

[1] https://crack.sh/

Triple DES (3DES)

- Cifra de bloco;
- Mais seguro do que o DES por usar uma chave maior;
- Texto claro dividido em blocos de 64 bits.
- Possui dois modos de funcionamento.
- Modo 1:
  - Criptografia do DES com a chave K_1;
  - Decriptografia do DES com a chave K_2;
  - Criptografia do DES com a chave K_1 novamente.
- Modo 2:
  - Criptografia do DES com a chave K_1;
  - Decriptografia do DES com a chave K_2;
  - Criptografia do DES com a chave K_3.

Blowfish

- Cifra de bloco;
- Foi um dos primeiros algoritmos não patenteados e é livre para qualquer pessoa usar sem restrições.
- Mais seguro do que o DES.
- Texto claro dividido em blocos de 64 bits.
- Chaves variam de 32 a 448 bits.
- Também possui 16 rodadas de substituições, mas são mais complexas do que o DES.

Twofish

- Cifra de bloco;
- Um dos finalistas da competição *Advanced Encryption Standard*.
- Evolução do Blowfish, recomendada atualmente pelo seu antigo autor, que também auxiliou no desenvolvimento do *Twofish*.
- Texto claro dividido em blocos de 128 bits.
- Chaves de até 256 bits.
- Também não é patenteado e é livre para qualquer pessoa usar sem restrições.

Advanced Encryption Standard (AES)

- Conhecido anteriormente como Rijndael.
- Vencedor da competição *Advanced Encryption Standard* e recomendado pelo NIST até hoje como padrão de segurança.
- Texto claro dividido em blocos de 128 bits.
- Chaves podem possuir 128, 192 ou 256 bits.
- Definido pelos padrões:
  - FIPS PUB 197: Advanced Encryption Standard (AES).
  - ISO/IEC 18033-3:: Block ciphers.

Advanced Encryption Standard (AES)

Tempo médio exigido para uma busca exaustiva no espaço de chaves (força bruta):

Tamanho de chave (bits)	Cifra	Número de chaves	Tempo exigido a 10^9 decriptações/s	Tempo exigido a 10^{13} decriptações/s
56	DES	$7,2 \times 10^{16}$	$1,125$ ano	1 hora
168	3DES	$3,7 \times 10^{50}$	$5,8 \times 10^{33}$ anos	$5,8 \times 10^{29}$ anos
128	AES	$3,4 \times 10^{38}$	$5,3 \times 10^{21}$ anos	$5,3 \times 10^{17}$ anos
192	AES	$6,3 \times 10^{57}$	$9,8 \times 10^{40}$ anos	$9,8 \times 10^{36}$ anos
256	AES	$1,2 \times 10^{77}$	$1,8 \times 10^{60}$ anos	$1,8 \times 10^{56}$ anos

Tempo desde a criação do Universo: $13,8 \times 10^9$ anos

Advanced Encryption Standard (AES)

- AES também é resistente a outros ataques, como ataques de aniversário (*Birthday Attacks*).
- *Birthday Attacks*: ataques que exploram a presença de colisões entre mensagens para descobrir a chave inicial.
- Colisões acontecem quando duas entradas diferentes produzem a mesma saída do algoritmo de criptografia.
- Número pequeno de tamanho de blocos aumentam as chances de acontecerem colisões.
- Exemplo:
  - Ataque Sweet32 permite quebra do 3DES com $2^{36,6}$ blocos (785 GB).
  - Experimentalmente, pesquisadores conseguiram obter colisões com 25 minutos apenas.

Exercício

Exercício 1

Assinale a alternativa que apresenta apenas algoritmos de criptografia de chave simétrica.

A) 3DES, AES e DES.

B) Diffie-Hellman, RSA e DES.

C) RSA, AES e IDEA.

D) AES, ElGamal e Diffie-Hellman.

E) Blowfish, ElGamal e IDEA.

Exercício

Exercício 2

Se uma cifragem baseia-se no uso de uma chave simétrica de 10 bits, além de podermos considerar a sua segurança como sendo "muito fraca", qual é a chance de um atacante quebrá-la na primeira tentativa de adivinhação?

A. 1/1024, uma chance em 1024.

B. 1/100, uma chance em cem.

C. 1/10, uma chance em dez.

D. 1/1048576, uma chance em (1024*1024).

E. 1/256, uma chance em 256.

Exercício

Exercício 3

Sobre os algoritmos de criptografia, considere as afirmativas a seguir.

I. O algoritmo DES (*Data Encryption Standard*) não é considerado seguro em sua forma original.

II. O algoritmo AES (*Advanced Encryption Standard*) é um algoritmo de chave simétrica.

III. A criptografia simétrica tem como objetivo garantir a confidencialidade.

IV. Os algoritmos de criptografia de chave simétrica manipulam chaves públicas e privadas.

Assinale a alternativa correta.

A) Somente as afirmativas I e IV são corretas.

B) Somente as afirmativas I e II são corretas.

C) Somente as afirmativas I, II e III são corretas.

D) Somente as afirmativas III e IV são corretas.

E) Somente as afirmativas II, III e IV são corretas.