Segurança e Auditoria de Sistemas

Criptografia

Criptografia

- Cifragem e decifragem
- Criptografia simétrica
- Criptografia assimétrica

Criptografia

- Usado para garantir a **confidencialidade** e **integridade** dos dados.
- Papel importante na **autenticação** de usuários e recursos.
- Origem grega *Kryptos* (oculto, secreto) e *graphos* (escrever)
- Objetivo:
  - Somente as pessoas autorizadas tem acesso a leitura.

Criptografia

- Elementos:
  - Texto aberto
  - Texto cifrado
  - Cifrador
  - Chaves criptograficas

Cifragem e decifragem

- Uma das mais antigas técnicas criptográficas conhecidas é o *cifrador de César*
- *Ex*

```
mensagem aberta:              Reunir todos os generais para o ataque
mensagem cifrada com k = 1: Sfvojs upept pt hfofsbjt qbsb p bubrvf
mensagem cifrada com k = 2: Tgwpkt vqfqu qu igpgtcku rctc q cvcswg
mensagem cifrada com k = 3: Uhxqlu wrgrv rv jhqhudlv sdud r dwdtxh
```

Cifragem e decifragem

- Para decifrar é necessario conhecer a chave K
- Ou tentar "quebrar" a mensagem
  - tentativa exaustiva ou "força bruta"
  - Para o cifrador de César existem somente 26 valores possíveis.
  - Chaves possíveis = espaço de chaves.
  - O segredo de uma técnica criptográfica **não** deve residir no algoritmo, mas no espaço de chaves.
    - AES(Advanced Encryption Standard) (Padrão governo americano) = chaves de 128 bits. Analisando 1 bilhão de chaves por segundo seria necessário 10 sextilhões de anos!

Cifragem e decifragem

- Representação de operação de:
  - Cifragem de um conteúdo **x** usando uma chave **k** = $\{x\}_k$
  - Decifragem de um conteúdo **x** usando uma chave **k** = $\{x\}_k^{-1}$

Criptografia simétrica

- O tipo da chave classifica a criptografia em:
  - simétrica e
  - assimétrica.
- Criptografia simétrica usa a mesma chave **k** para cifrar e decifrar a informação.

$$\{\{x\}_k\}_{k'}^{-1} = x \leftrightarrow k' = k$$

Criptografia simétrica

- Exemplos:
  - Cifrador de César
  - DES (Data Encryption Standard)
  - AES (Advanced Encryption Standard)

- **Problema**: Se enviar a mensagem cifrada para alguém ele tem que conhecer a chave.

Criptografia assimétrica

- Algoritmos assimétricos usam um par de chaves complementares:
  - Uma chave pública kp
  - Uma chave privada kv

$$\{\{x\}_{kp(u)}\}_{kv(u)}^{-1} = x$$

$$\{\{x\}_{kv(u)}\}_{kp(u)}^{-1} = x$$

Criptografia assimétrica

- Exeplos:
  - RSA (Rivest-Shamir-Adleman)
  - Diffie-Hellman

- Pode ser usado para identificar a autoria.
  - Assinatura digital.

Criptografia assimétrica

- Mais versáteis
- Mais processamento
- Muito usado associado a simétricos.
  - Ex: TLS(Transport Layer Security) usado para SSH e HTTPS.