Tópicos em Redes de Computadores

Aula de Hoje:

Criptografia

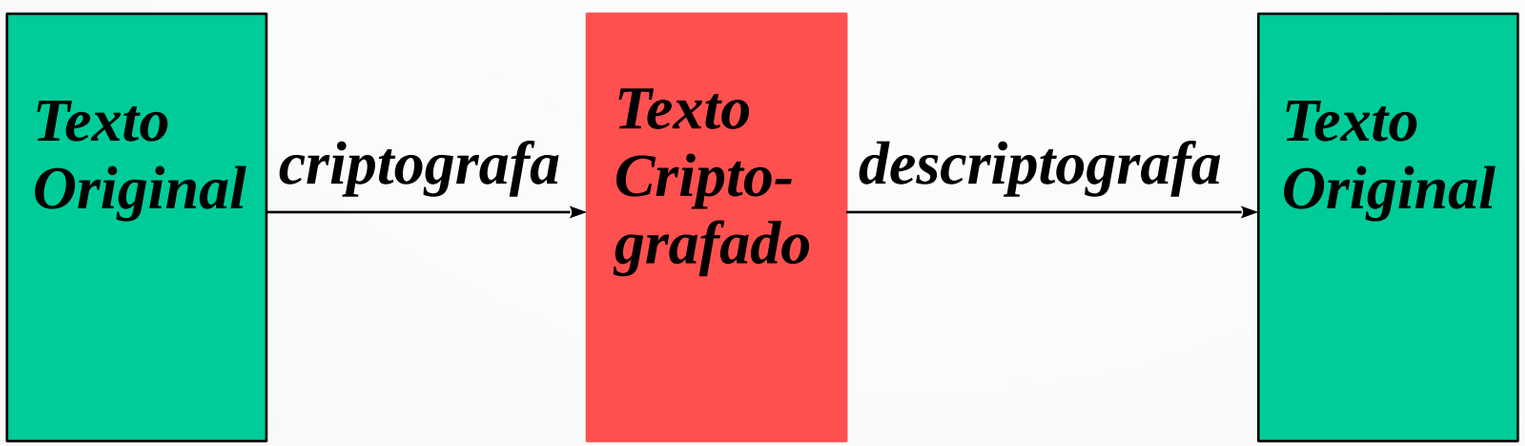
Prof. Elias P. Duarte Jr.
Universidade Federal do Paraná (UFPR)
Departamento de Informática
www.inf.ufpr.br/elias/topredes

Sumário

- O que é criptografia?
- Substituição & Transposição
- Criptografia de Chave Secreta
- Criptografia de Chave Pública
- Resumo Digital ou Hash
- Ataques & Quebra de Códigos

O Que É Criptografia?

- A palavra vem do grego: segredo + escrita
- Arte da escrita secreta
- Esquema geral:



Informação Criptografada

- O texto criptografado é aparentemente uma sequência de caracteres aleátorios, sem nenhum sentido
- Só quem conhece o algoritmo e a chave utilizados pode descriptografar
- Desta forma: a informação flui entre emissor e receptor sem que nenhuma parte não autorizada possa acessar o conteúdo

Em outras palavras:

- Seja T o texto original da mensagem;
- Seja $C_k( )$ o algoritmo de critpografia, parametrizado pela chave k
- $C_k(T)$ é então o texto criptografado
- Seja $D_k( )$ o algoritmo para descriptografar, ele usa a mesma chave k; então:

$$T = D_k(C_k(T))$$

Para que serve a criptografia?

- Além de permitir o armazenamento e comunicação de informações sigilosas,
- A criptografia também é usada para garantir:
  - a integridade de uma mensagem
  - a autenticidade de um usuário (ou processo)

Algoritmos & Chaves

- Criptografia envolve um algoritmo e um valor secreto - a chave
- O algoritmo é muitas vezes público
- Assim, podemos dizer que os algoritmos são parametrizados pela chave secreta
- Não é trivial obter um bom algoritmo de criptografia

Fácil & Difícil

- Um algoritmo de criptografia deve ser razoavelmente eficiente para que seus usuários legítimos possam usá-lo
- Por outro lado, para os criminosos, deve ser computacionalmente inviável descobrir o texto original a partir do criptografado
- Nem só criminosos: cripto-analistas

Computacionalmente Difícil

- É sempre possível tentar testar todas as chaves até encontrar a correta
- Entretanto, se fazê-lo demoraria por exemplo 10 mil anos usando todos os computadores existentes na Terra, temos um bom algoritmo de criptografia
- O número de bits da chave é um fator importante neste sentido

Comprimento da Chave

- 1 dígito => 10 possibilidades
- 2 dígitos => 100 possibilidades
- 3 dígitos => 1000 possibilidades
- 6 dígitos => 1000000 possibilidades
- Possibilidades crescem exponencialmente
- Para e-mail seguro: chaves de 64 bits OK
- Para aplicações militares: no mínimo 512 bits

Algoritmos Públicos

- Uma boa estratégia para testar um algoritmo é publicá-lo
- Diversos cripto-analistas de todo o mundo vão testar o algoritmo de graça
- Por outro lado, se além da chave, o algoritmo também for secreto, pode ficar mais difícil quebrar um código
- Entretanto: é difícil manter segredo sobre um algoritmo muito usado

Algoritmos Secretos

- Hoje em dia, algoritmos de criptografia secretos em geral são das forças armadas
- Os sistemas comerciais usam algoritmos publicados - mas são **bons** algoritmos

Sustituição & Transposição

- Todos os algoritmos de criptografia são baseados nestes dois princípios
- Estes métodos têm sido usados, na sua forma mais simples, desde a antiguidade
- São também encontrados em revistas de passatempo e jornais...

Substituição

- Consiste em substituir cada letra ou grupo de letras por outra letra ou grupo
- Considere o mapeamento A->S, M->A, E->B, I->I, X->O
- AMEIXA
- Pode substituir palavras, sílabas também
- O Método de César, usado pelo imperador romano é um exemplo típico

Substituição

- Consiste em substituir cada letra ou grupo de letras por outra letra ou grupo
- Considere o mapeamento A->S, M->A, E->B, I->I, X->O
- SABIOS
- Pode substituir palavras, sílabas também
- O Método de César, usado pelo imperador romano é um exemplo típico

O Método de César

- Atribuído ao imperador romano Júlio César
- É uma substituição de letras, a -> D, b -> E, c-> F,....., z -> C
- Por exemplo: APRENDER
- Há uma chave, que é o deslocamento, no caso acima k=3
- Para descriptografar é necessário saber o deslocamento, isto é, a chave

O Método de César

- Atribuído ao imperador romano Júlio César
- É uma substituição de letras, a -> D, b -> E, c-> F,....., z -> C
- Por exemplo: DSUHQGHU
- Há uma chave, que é o deslocamento, no caso acima k=3
- Para descriptografar é necessário saber o deslocamento

Será Difícil Quebrar o Método?

- Como fazer para descobrir a chave usada?
- Lembre-se: sempre é possível tentar testar todas as possibilidades
- Neste caso, são quantas possibilidades?
- Resposta: 26
- Tente quebrar o código do texto no qual aparece:
  ZLNBYHUJH
- Qual a chave usada?

Será Difícil Quebrar o Método?

- Como fazer para descobrir a chave usada?
- Lembre-se: sempre é possível tentar testar todas as possibilidades
- Neste caso, são quantas possibilidades?
- Resposta: 26
- Tente quebrar o código do texto no qual aparece:
  SEGURANÇA
- Qual a chave usada? K=7

Substituição Monoalfabética

- Para melhorar o método da substituição
- Idéia: substituir cada letra por outra aleatória
- O que é a chave neste caso?
- A sequência de 26 caracteres do mapeamento

Substituição Monoalfabética: Exemplo

- Podemos fazer o seguinte mapeamento:
- ABCDEFGHIJKLMNOPQRSTUVWXYZ
- KRMZWATDCEVJFGBHILNOPQSUXY
- A segunda sequência é a chave
- Neste caso, quantas possibilidades devem ser testadas no total?
- Resposta: $26! \sim 4x10^{26}$
- Testando uma possibilidade por micro-segundo: 1013 anos

Quebrando a Substituição Monoalfabética

- O que será a palavra abaixo?
- LWZWN
- Solução:
- Busca de palavras prováveis, e padrões prováveis
- Exemplo: em inglês as letras mais comuns são e, t, o, a, n, i, ..., nesta ordem

Quebrando a Substituição Monoalfabética

- O que será a palavra abaixo?
- LWZWN
- Solução: REDES
- Busca de palavras prováveis, e padrões prováveis
- Exemplo: em inglês as letras mais comuns são e, t, o, a, n, i, ..., nesta ordem

Propriedades Estatísticas das Linguagens Naturais

- Deve-se começar procurando a letra mais comum, por exemplo ‘‘e’’ (em inglês)
- Depois pode-se procurar a segunda letra mais comum “t”
- Se houverem muitos “tXe”, provavelmente X -> h, e então “thZt” Z-> a
- A busca de palavras prováveis em um documento específico é outra boa estratégia

Transposição

- Neste método, as letras são reordenadas, trocadas de lugar, mas não são substituídas
- Assim, a transformação seguinte pode ocorrer AMEIXA
- Trocamos as letras da palavra de lugar, seguindo um algoritmo que permite a volta
- A chave neste caso foi a palavra CHAVES

Transposição

- Neste método, as letras são reordenadas, trocadas de lugar, mas não são substituídas
- Assim, a transformação seguinte pode ocorrer EAXMAI
- Trocamos as letras da palavra de lugar, seguindo um algoritmo que permite a volta
- A chave neste caso foi a palavra CHAVES

Transposição por Colunas

- Nesta transposição fizemos:

C	H	A	V	E	S
2	4	1	6	3	5
A	M	E	I	X	A

Transposição por Colunas

- Para descriptografar:

C	H	A	V	E	S
2	4	1	6	3	5
E	A	X	M	A	I

Transposição por Colunas

- A chave não pode conter letras repetidas
- Usando-se a chave, as colunas são numeradas pela ordem léxica das letras da chave; a letra mais próxima do início do alfabeto = 1, etc.
- Para descriptografar, basta fazer um mapeamento de posições

Transposição - Descriptografando

- Assim, no exemplo anterior, “X’’ está agora na terceira posição, aquela da letra A-1, mas a terceira letra é a letra E, que está na quinta posição, é a posição correta de “X”

1	**2**	**3**	**4**	**5**	**6**
C	**H**	**A**	**V**	**E**	**S**
2	**4**	**1**	**6**	**3**	**5**
E	**A**	**X**	**M**	**A**	**I**

Transposição: Exercício

- Criptografar e Descriptografar a palavra SEGURO com a chave CHAVES

1	2	3	4	5	6
C	H	A	V	E	S
2	4	1	6	3	5
S	E	G	U	R	O

Transposição: Exercício

- Lembre-se a letra que está na posição da 1a letra da chave deve ir para a posição da 3a letra

Transposição: Exercício

- Lembre-se a letra que está na posição da 1a letra da chave deve ir para a posição da 3a letra

1	2	3	4	5	6
C	H	A	V	E	S
2	4	1	6	3	5
G	S	R	E	O	U

Transposição de Textos

- No caso de um texto, procedemos da seguinte forma:

1 2 3 4 5 6
CHAVES
2 4 1 6 3 5
ESTE É U
MEXEMP
LOD ETR
ANS POS
I ÇÃO

Transposição de Textos

- O texto:
- ESTEÉUMEXEMPLODETRANSPOSIÇÃO
- Se transforma em:
- TXDSÃEMLAIEMTOSEONÇUPRSEEEPO
- Descriptografar como exercício!

Quebrando a Transposição

- Usando as propriedades estatísticas das linguagens naturais -> frequência de sílabas...
- Depois é necessario descobrir quantas colunas existem -> onde é que as letras de uma palavra provável se encontram?

S E G
U R O

S E
GU
RO

Concluindo a Transposição

- Depois de descobrir o número de colunas, é necessário ordená-las
- Para uma chave pequena, não é difícil tentar todas as possibilidades
- Outro método de transposição: criptografa um bloco fixo de caracteres, e tem a ordem
- Exemplo: 4 caracteres, ordem = 3241

One Time Pad: Um Método Poderoso

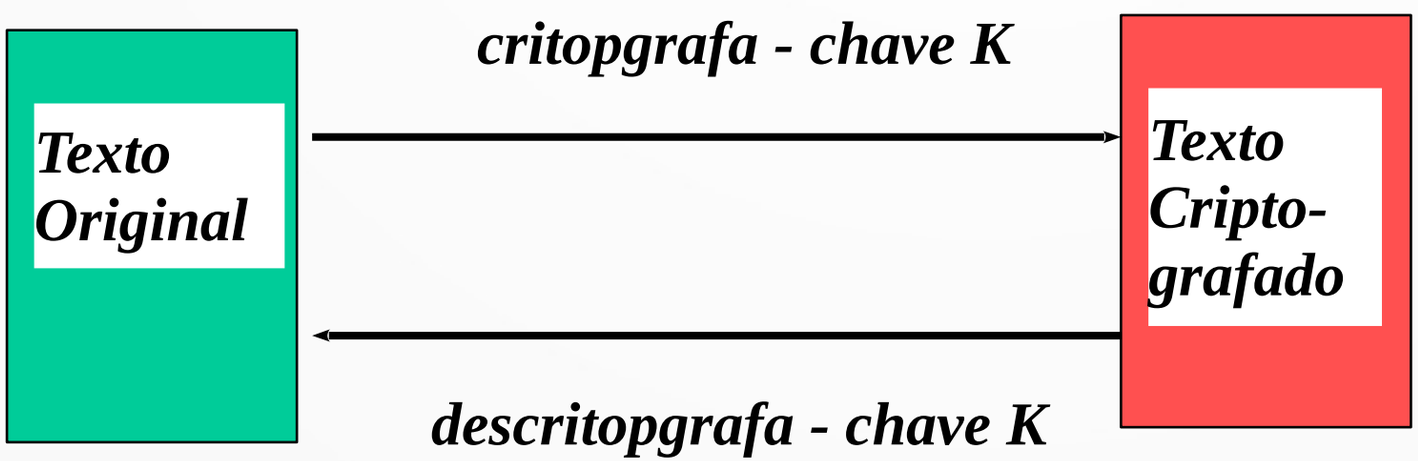
- Basta que a chave seja uma sequência totalmente aleatória de bits do tamanho exato da mensagem a ser transmitida
- É feito um XOR (ou-exclusivo) da mensagem com a chave
- Por exemplo: 1010 xor 0011 = 1001
- Neste caso todo bit é aleatório!
- Problemas: transmitir msg+nova chave

Os Três Tipos de Criptografia

- *Criptografia de Chave Secreta*
- *Critografia de Chave Pública*
- *Resumo Digital ou Hash*

Criptografia de Chave Secreta

- Envolve o uso de uma única chave
- O algoritmo para descriptografar é o reverso do algoritmo para criptografar

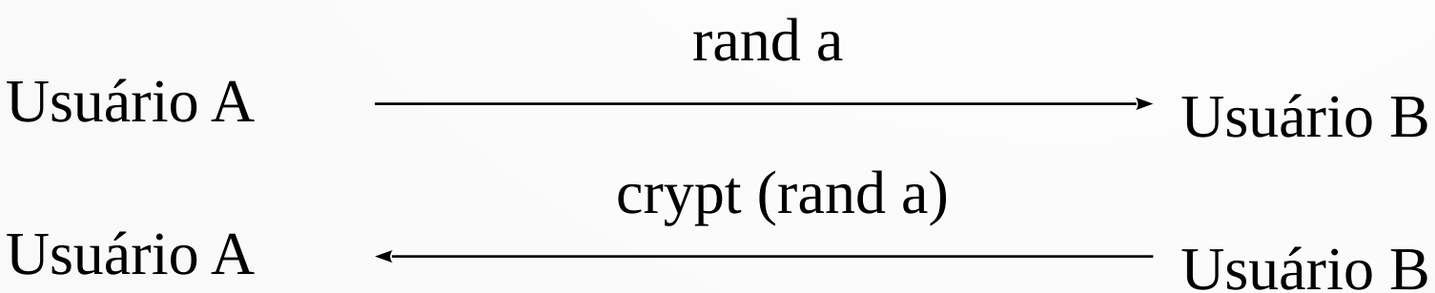


Usos de Criptografia de Chave Secreta

- Para manter o sigilo de informações transferidas em canal inseguro
- Para armazenar informações sigilosas
- Cuidado! Se você esquecer a chave as informações estarão irremediavelmente perdidas!
- Checagem de Integridade
- Checksums secretos

Usos de Criptografia de Chave Secreta

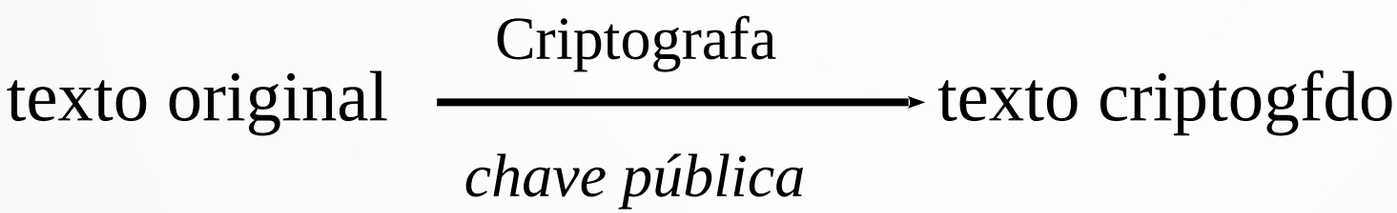
- Autenticação
- Um usuário (ou processo) pode provar sua identidade
- Usado em desafios do tipo:

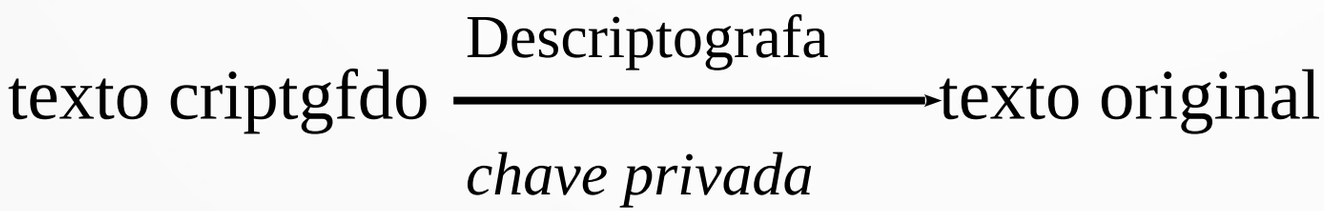


Criptografia de Chave Pública

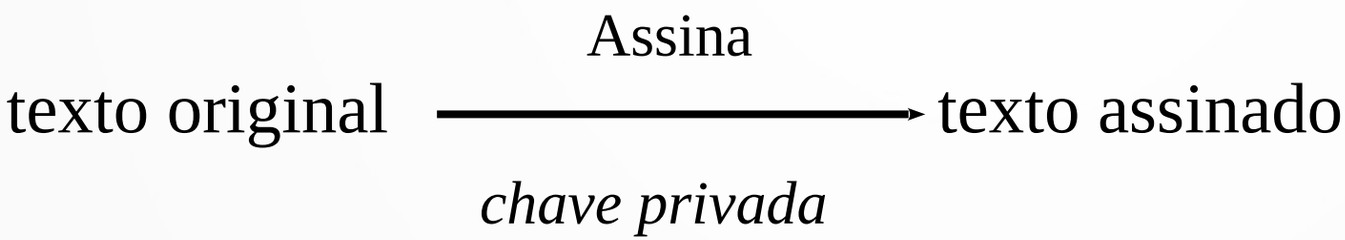
- Chamados assimétricos, enquanto os algoritmos de chave secreta são simétricos
- Todos os usuários tem DUAS chaves:
- Chave Pública, conhecida por todos
- Chave Privada, que não é distribuída
- O texto é criptografado com uma chave e descriptografado com a outra!

Criptografia de Chave Pública





Criptografia de Chave Pública: Assinando Mensagens



Usos da Criptografia de Chave Pública

- Para armazenar informações sigilosas: deve-se criptografar com a chave pública (não com a privada)
- Para transferir mensagens sigilosas -> emissor criptografa com a chave pública do receptor
- Autenticação: desafio deve ser criptografado com a chave pública
- Assinatura de mensagens

Resumo Digital ou Hash

- Não usam chave alguma!
- Os algoritmos em si não são secretos
- Mas são usados em segurança!!
- É uma função matemática que
  - recebe uma entrada de tamanho arbitrário
  - produz um número (pequeno, 128 ou 160 bits são comuns) como saída
- É possível que várias mensagens gerem o mesmo hash, mas deve ser difícil encontrar tal par

Usos do Hash

- Armazenamento de passwords: o sistema guarda o hash, não a senha!
- Geração de assinaturas digitais
- Geração de checksums
- Antídotos de vírus
- Os algoritmos de hash são mais eficientes que os algoritmos de chave pública

Ataques e Quebra de Algoritmo

- A partir de Texto Criptografado
  - o texto criptografado estando disponível
  - o objetivo é descobrir o texto original
  - quando é que se sabe que se achou tal texto?
- A partir de <Txto Original, Txto Criptgfd>
  - um espião conseguiu obter um par
  - em alguns casos (subst. monoalf.) tudo perdido!
- Texto Escolhido pelo Hacker

Conclusão

- Definição de Criptografia
- Substituição & Transposição
- Criptografia de Chave Secreta, Pública & Hash
- Ataques

Obrigado!

Lembrando: a página da disciplina é:
https://www.inf.ufpr.br/elias/topredes