Tópicos em Redes de Computadores

Criptografia de Chave Pública

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

Sumário

- Criptografia de Chave Pública: Definições & Usos
- Aritmética Modular
- O Algoritmo RSA

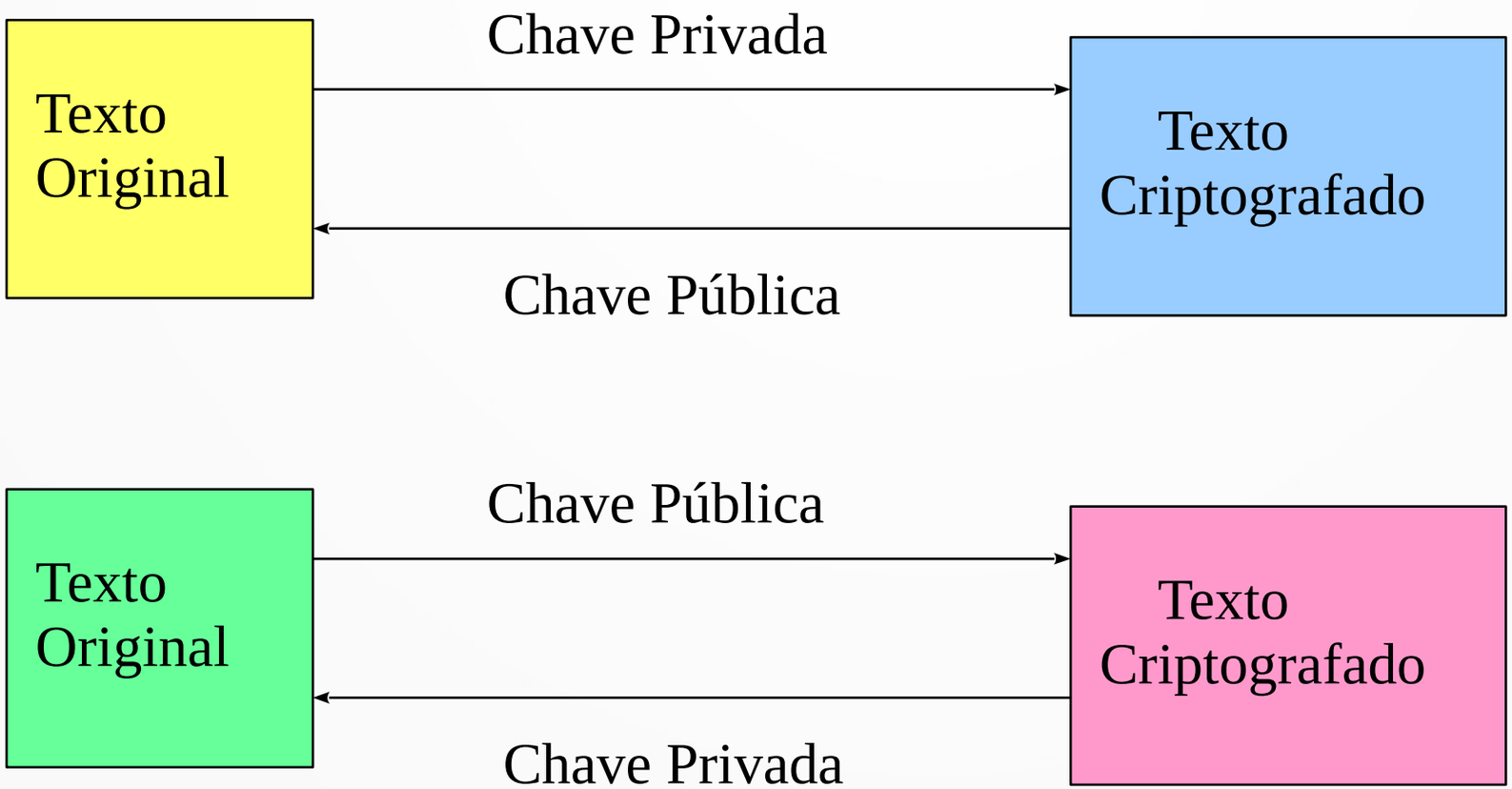
Distribuição de Chave Secreta

- Na criptografia de chave secreta: o maior problema é a chave DEIXAR de ser secreta
- Ambos origem e destino usam a mesma chave secreta!
- Risco: como compartilhar e distribuir a chave?
- Se a chave for descoberta por um invasor, por melhor que seja o algoritmo, está tudo perdido

Que tal usar chaves públicas?

- Na criptografia de chave pública, todos conhecem uma das chaves! É distribuída publicamente
- Proposta originalmente em 1976, por Diffie & Hellman (que têm um protocolo de compartilhamento de chave secreta)
- O sistema usa duas chaves diferentes: uma para criptografar, outra para descriptografar
- Todos conhecem uma das chaves! É distribuída publicamente

Duas Chaves


Texto Original
Chave Privada
Texto Criptografado
Chave Pública
Texto Original
Chave Pública
Texto Criptografado
Chave Privada

Duas Formas de Uso

- Bob criptografa uma mensagem para Alice com a chave pública da Alice
- Apenas Alice consegue descriptografar, com sua chave privada

- Bob criptografa mensagem para Alice com a chave privada dele próprio (de Bob)
- Ao usar a chave pública de Bob para descriptografar a mensagem, Alice confirma sua origem

Todo mundo conhece a chave...

- Critptografia de chave pública é também chamada de criptografia assimétrica
- Pois há duas chaves envolvidas, uma diferente da outra
- Criptografia de chave secreta é também chamada de criptografia simétrica
- Uma única chave é usada para criptografar E descriptografar

Criptografia Assimétrica

- DescriptK1(CriptK2(P)) = P
- Deve ser extremamente difícil obter uma das chaves a partir da outra
- Como uma das chaves é pública, e o algoritmo também é público, o intruso pode tentar realizar vários experimentos para descobrir a chave privada

Um Pouco de Matemática

- Aritmética Modular
- Módulo n
- x mod n é o resto da divisão inteira de x por n
- Inclui apenas os números inteiros menores ou iguais a n

Soma Módulo n

- Basta tirar o módulo n do resultado
- Exemplos módulo 10:
- 5 + 5 = 0
- 3 + 9 = 2
- 2 + 2 = 4
- 9 + 9 = 8
- Na verdade o método de César usa soma módulo 26 considerando o alfabeto

Subtração Módulo n

- Seja -i o número que você tem que somar a i para obter 0
- Considere o número 7; -7 = 3

Um Método com 2 Chaves!

- A soma módulo n faz o mapeamento:
  - 0 1 2 3 4 5 6 7 8 9
- Criptografa com chave 8 (soma 8 módulo 10):
  - 8 9 0 1 2 3 4 5 6 7
- Descriptografa com a chave 2 (soma -8=2 mod 10):
  - 0 1 2 3 4 5 6 7 8 9
- Uma chave (8) é usada para criptografar, outra (2) é usada para descriptografar!

Multiplicação Módulo n

- Como fica a tabela de múltiplicação módulo 10 quando multiplicamos por 0?
  - 0 1 2 3 4 5 6 7 8 9
  - 0 0 0 0 0 0 0 0 0 0
- Quando multiplicamos por 1?
  - 0 1 2 3 4 5 6 7 8 9
  - 0 1 2 3 4 5 6 7 8 9

Multiplicação Módulo 10

- Agora vamos multiplicar por 3
  - 0 1 2 3 4 5 6 7 8 9
  - 0 3 6 9 2 5 8 1 4 7
  - **Mapeamento perfeito!!**
- Multiplicando por 6:
  - 0 1 2 3 4 5 6 7 8 9
  - 0 6 2 8 4 0 6 2 8 4
  - Neste caso cada dois números são mapeados para a mesma saída
  - **Há perda de informação**

Prepare a Tabela Completa

Prepare a Tabela Completa

	0	1	2	3	4	5	6	7	8	9
0 ->	0	0	0	0	0	0	0	0	0	0
1 ->	0	1	2	3	4	5	6	7	8	9
2 ->	0	2	4	6	8	0	2	4	6	8
3 ->	0	3	6	9	2	5	8	1	4	7
4 ->	0	4	8	2	6	0	4	8	2	6
5 ->	0	5	0	5	0	5	0	5	0	5
6 ->	0	6	2	8	4	0	6	2	8	4
7 ->	0	7	4	1	8	5	2	9	6	3
8 ->	0	8	6	4	2	0	8	6	4	2
9 ->	0	9	8	7	6	5	4	3	2	1

Quais Chaves Podemos Usar?

Quais Chaves Podemos Usar?

- Apenas {1, 3, 7, 9}
- Por que?
- Estes números e o 10 são primos entre si
- O único divisor comum entre estes números e o 10 é 1

Inverso Multiplicativo

- Considere o número x
- Qual outro número eu devo multiplicar por x para obter 1?
- Este é o inverso multiplicativo de x (x_{-1})
- $x * x_{-1} = 1$
- Apenas os números {1, 3, 7, 9} têm inversos multiplicativos módulo 10

Inversos Multipc Módulo 10

- Confira sua tabela!
- O inverso de 9 e de 1 são 9 e 1, respectivamente ;-)
- O inverso de 7 é 3
- Assim temos DUAS CHAVES!
- Veja que {1,1} e {9,9} não são nem diferentes (mesma chave) nem são um bom par de chaves...
- Entretanto {3,7} fazem um mapeamento com muito boa aparência!

Obtendo o Inverso

- Considerando os números de 1 dígito é fácil testar todas as possibilidades
- Considerando números GRANDES, por exemplo de 100 dígitos, é difícil descobrir o inverso usando a força bruta
  - “difícil” → computacionalmente difícil
- O algoritmo de Euclides é usado para descobrir (tendo x e n) o número y tal que x*ymod n =1
- O algoritmo de Euclides é eficiente!

O Algoritmo de Euclides

- Para calcular o MDC de dois números i,j
- Publicado no livro Elementos, de Euclides, há mais de 2000 anos!

```
while (i>0) {
 if (i<j)
    {t=i; i=j; j=t; }
 i = i-j;
}
```

Exponenciação Módulo n

- Usa os mesmos princípios da adição e multiplicação
- ... após efetuar a operação a^b é obtido o mod n
- Em alguns casos é possível obter o inverso da exponenciação

O Algoritmo RSA

- Proposto por Rivest, Shamir e Adleman na década de 1970
- Este algoritmo é baseado nos seguintes princípios:
- Selecione dois números primos grandes (p,q)
- Calcule n = p*q, z = (p-1)*(q-1)
- Escolha d, sendo d,z primos entre si
- Descubra ‘e’ tal que e*d = 1 mod z
  - Ou seja ‘e’ é o inverso multiplicativo de d mod z

RSA Cripto & Descriptografando

- Para criptografar a mensagem P
- Faça $C = P^e \pmod n$
- Para descriptografar
- Faça $P = C^d \pmod n$
- Desta forma, o RSA é baseado em exponenciação modulo n
- d é o inverso multiplicativo de e módulo n

RSA: Chaves

- Para criptografar é necessário saber (e,n)
- Para descriptografar é necessário saber (d,n)
- Chave pública (e,n)
- Chave privada (d,n)
- A dificuldade em descobrir d a partir de (e,n) está em fatorar números grandes (ex. 100 dígitos)

RSA: Um Exemplo

- Vamos criptografar a letra S (cod 19)
- Vamos usar dois primos pequenos:
- p=3, q=11 desta forma n=p*q=33
- z=(p-1)(q-1)=20
- Podemos escolher d=7 pois (7,20) são primos entre si
- Escolhemos e=3, pois 7*e=1 mod 20

RSA: Continuação do Exemplo

- Criptografando: $C = 19^3 \bmod 33 = 28$
- Descriptografando: $P = 28^7 \bmod 33 = 19$
- Neste exemplo é fácil fatorar n=33 e obter p,q e então z
- Conhecendo z, e conseguimos obter d usando o algoritmo de Euclides

Fatorando Números Grandes

- Considerando um tempo médio por instrução de 1 microsegundo:
- Para fatorar um número de 200 dígitos seriam necessários 4 bilhões de anos
- 500 dígitos -> 10^{25} anos!
- Mesmo considerando tempos por instrução ordens de magnitude menor (1 nanosegundo é a realidade de hoje) é necessário muito tempo para fatorar

Outros Algoritmos

- RSA é o algoritmo de criptografia de chave pública mais usado no mundo
- Existem vários outros algoritmos
- O primeiro algoritmo de chave pública era baseado no problema da mochila, e foi proposto por Merkle and Hellman
- A lista de todos os objetos para colocar na mochila é pública, os pesos dos objetos selecionados também
- Entretanto a seleção de objetos é secreta

Outros Algoritmos – cont.

- O inventor do algoritmo estava tão certo da sua segurança que ofereceu publicamente US$100 a quem conseguisse quebrá-lo
- Isso foi feito imediatamente por Adi Shamir (o “S” do RSA)
- O inventor propôs modificações e ofereceu US$1000 a quem conseguisse quebrá-lo
- Rivest (o “R” do RSA) levou o prêmio!

Conclusão

- Estudamos os algoritmos de criptografia com chave pública
- Entendemos porque usamos duas chaves, e porque uma delas pode ser pública
- Operações aritméticas módulo n
- O Algoritmo RSA

Obrigado!

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