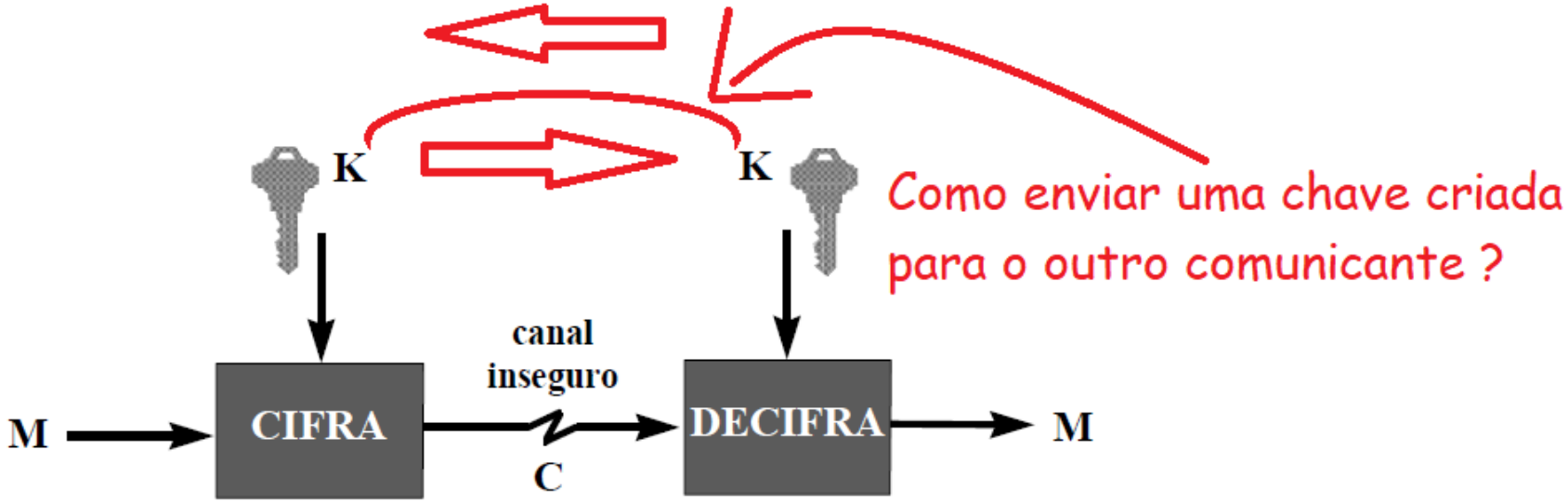
Sistemas criptograficos assimétricos

Prof. Rogério Leão S. de Oliveira

Sistemas criptograficos assimétricos

Criptografia assimétrica - surgimento

- Gerenciamento das chaves secretas do sistema simétrico é um desafio.
- A geração, transmissão e armazenamento dessas chaves é um trabalho complexo, principalmente em ambientes abertos como a internet.
- Surge então o sistema assimetrico para resolver esse problema.



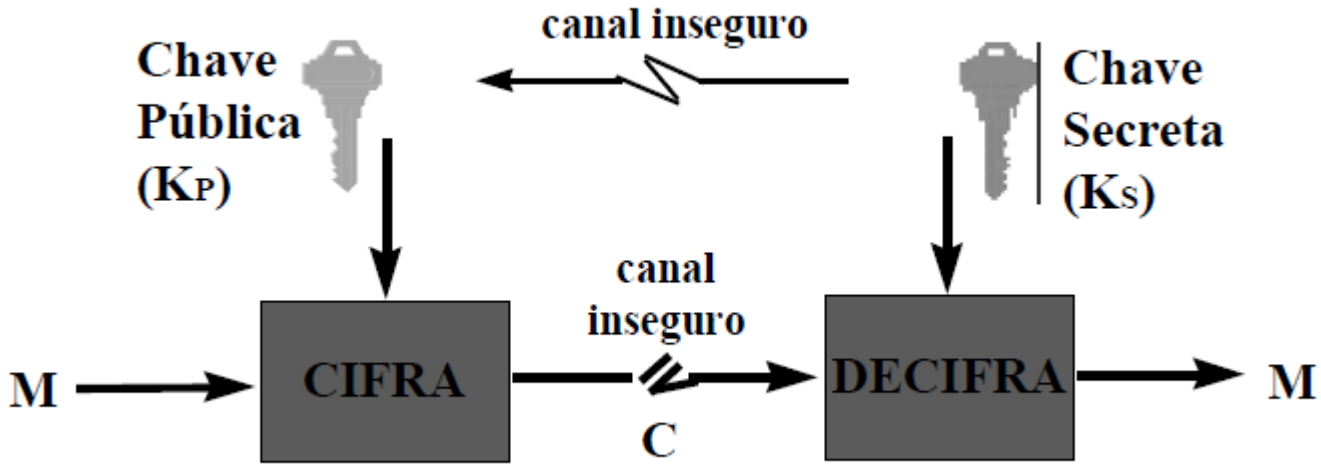
Sistemas criptograficos assimétricos

Criptografia assimétrica - fundamentos

- Cada participante possui um par de chaves (uma chamada de pública e a outra chamada de privada ou secreta).
- A chave publica é aberta a todos e portanto deve ser divulgada aos interessados em comunicar-se com o dono daquela chave.
- A chave privada, ao contrário, deve ser conhecida exclusivamente pelo seu proprietário e portanto armazenada com segurança.
- A chave publica pertencente a um ente é gerada a partir da chave privada desse mesmo ente, sendo assim totalmente dependentes uma da outra (algébra), de modo que uma informação cifrada com a chave publica só pode ser decifrada com a respectiva chave privada.

Sistemas criptograficos assimétricos

Criptografia assimétrica - fluxo



Sistemas criptograficos assimétricos

Criptografia assimétrica - características

- Um dos problemas deste tipo de criptografia é a derivação/descoberta da chave privada a partir da chave publica(conhecida por todos).

- Para evitar este tipo de ataque, os algoritmos utilizados na geração realizam calculos matemáticos tão complexos e imensos que computacionalmente esta derivação se torna inviável.

Sistemas criptograficos assimétricos

Criptografia assimétrica - características

- Uma boa característica deste sistema de criptografia é que a chave secreta(privada) não precisa ser transmitida o que diminui significativamente a probabilidade de perdê-la.

- Em contrapartida, uma caracteristica negativa deste sistema é detectada no desempenho das cifragens e decifragens que são afetadas devido ao uso de calculos complexos e de grande volume de informação.

Sistemas criptograficos assimétricos

RSA.

- O RSA foi criado por Rivest, Shamir e Adleman, utiliza sua base matemática na dificuldade de fatorar dois números primos e pode ser implementado em diversas linguagens de programação.

- O Openssl é um sistema gratuito que implementa diversos tipos de algoritmos, inclusive o RSA. Então vamos aprendê-lo.

Sistemas criptograficos assimétricos

RSA – Gerando as chaves

A forma mais simples para gerar uma chave RSA é usar o comando da seguinte forma:

```
openssl genrsa -out nome_chave_privada [num_bits]
```

nome_chave_privada = substitua pelo nome do arquivo que conterá a chave;

[num_bits] = insira o numero de bits (tamanho) da chave.

Ex:

```
openssl genrsa –out rogerio.privada 1024
```

Sistemas criptograficos assimétricos

RSA – Gerando as chaves

É também possível encriptar a chave com uma palavra/frase secreta, de forma que a chave privada RSA não possa ser usada sem o conhecimento dessa palavra/frase(senha).

```
openssl genrsa -des3 -out rsa_key_file 1024
```

-des3 = parâmetro define que após o comando uma senha seja solicitada.

Sistemas criptograficos assimétricos

RSA – Gerando as chaves

A partir da chave privada RSA gerada anteriormente, pode-se (e deve se) gerar uma chave pública. Para isso usa-se o parâmetro **–pubout**:

```
openssl rsa -in rogerio.privada –pubout -out rogerio.publica
```

rogerio.privada = substitua pelo nome do arquivo que contem a chave privada;

rogerio.publica = substitua pelo nome do arquivo que conterá a chave pública.

Sistemas criptograficos assimétricos

RSA – Cifrando

```
openssl rsautl -encrypt -in msg.txt -pubin -inkey
  chave.publica -out cifrado.txt
```

msg.txt = substitua pelo nome do arquivo que contem o texto a ser cifrado;

chave.publica = substitua pelo nome do arquivo que contem a chave publica;

cifrado.txt = substitua pelo nome do arquivo que conterá o texto cifrado (resultado).

Sistemas criptograficos assimétricos

RSA – Decifrando

```
openssl rsautl -decrypt -in cifrado.txt -inkey
  chave.privada -out decifrado.txt
```

cifrado.txt = substitua pelo nome do arquivo que contem o texto a ser decifrado;

chave.privada = substitua pelo nome do arquivo que contem a chave privada;

decifrado.txt = substitua pelo nome do arquivo que conterá o texto decifrado (resultado);

Sistemas criptograficos assimétricos

RSA – Exercícios

- Crie seu par de chaves;
- Crieum arquivo texto e faça uma pergunta curta ao professor;
- Cifre essa pergunta de modo que somente o professor consiga decifra-la;
- Seguinte as demais orientações do professor envie para ele os arquivos necessários, inclusive para que ele te responda cifrado e você consiga decifrar.