Segurança da Informação– GBC083

Prof. Rodrigo Sanches Miani – FACOM/UFU

Aulas passadas

Segurança da Informação– GBC083

O que vimos até o momento?

- Princípios de segurança da informação;
  - Confidencialidade, Integridade e Disponibilidade
- Modelos clássicos de criptografia;
- Criptografia simétrica
  - Cifras de bloco: DES, AES
  - Modos de cifra de bloco: ECB, CBC, OFB...

O que vimos até o momento?

- O que ainda não foi visto?
- É possível usar um modelo de criptografia inteiramente baseado em um sistema simétrico? Qual a principal limitação disso?

Tópicos da aula

Segurança da Informação– GBC083

Tópicos da aula – Criptografia de chave pública

1. Motivação
2. Princípios
3. Requisitos
4. Aplicações
5. Criptoanálise

Motivação

Segurança da Informação– GBC083

Evolução - criptografia

- O desenvolvimento da criptografia de chave pública é a maior e talvez a única verdadeira revolução na história inteira da criptografia;
  - Turing award 2002 e 2015 - https://amturing.acm.org/byyear.cfm

- Praticamente todos os sistemas criptográficos têm sido baseados nas ferramentas elementares da substituição e permutação.

Evolução - criptografia

A criptografia de chave pública oferece uma mudança radical de tudo o que foi feito antes;

1. Os algoritmos de chave pública são baseados em **funções matemáticas**, em vez de substituição e permutação;

2. A criptografia de chave pública é **assimétrica**, envolvendo o uso de **duas** chaves separadas, ao contrário da criptografia simétrica, que utiliza apenas uma chave.

Motivação – criptografia assimétrica

O conceito de criptografia de chave pública evoluiu de uma tentativa de atacar um dos problemas mais difíceis associados à criptografia simétrica.

Que problema é esse?

Motivação – criptografia assimétrica

O conceito de criptografia de chave pública evoluiu de uma tentativa de atacar um dos problemas mais difíceis associados à encriptação simétrica.

Que problema é esse?

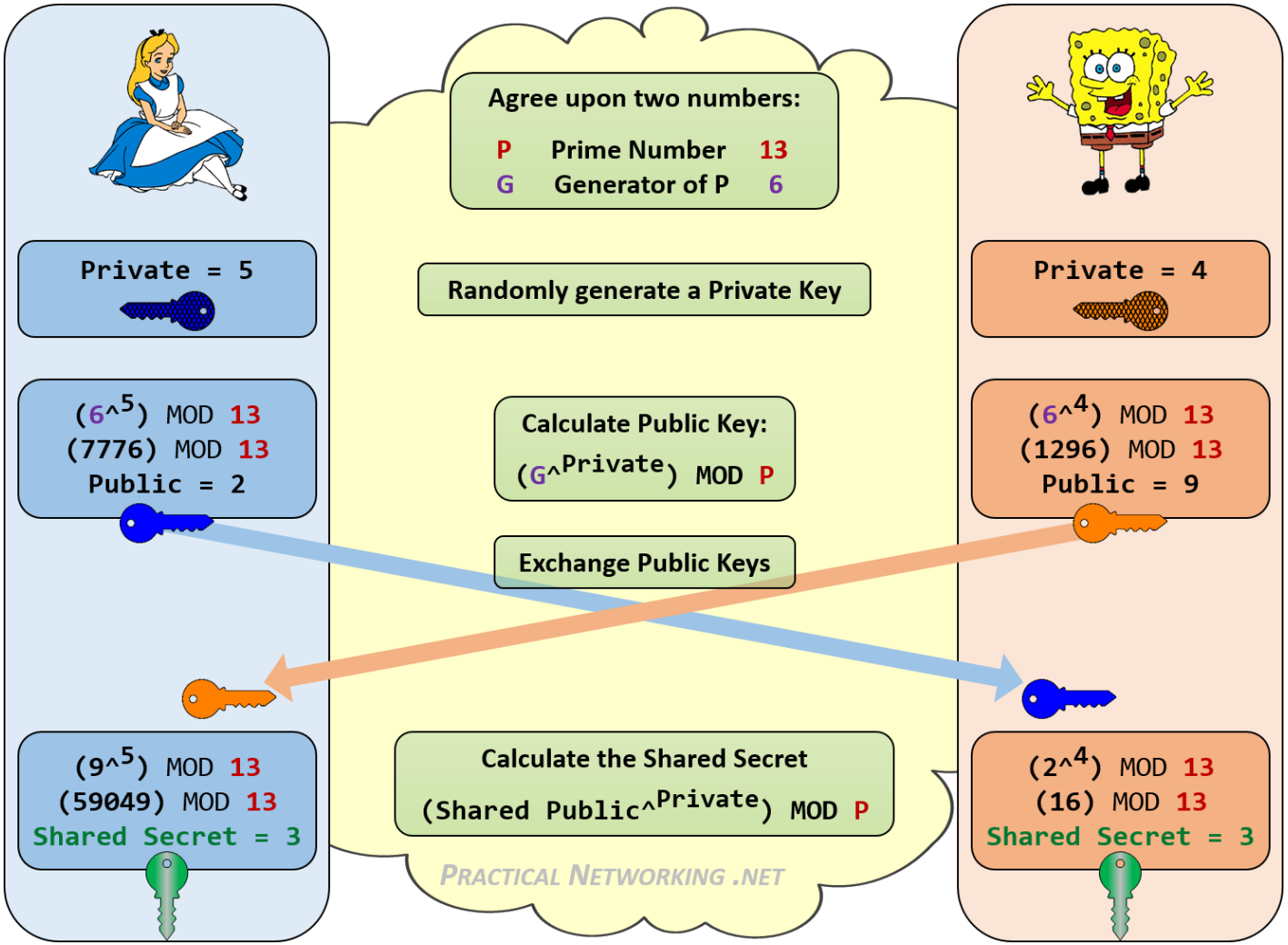
Resposta: troca de chaves!

Motivação – Diffie-Hellman

- O primeiro algoritmo de chave pública apareceu no artigo inicial de Whitfield Diffie e Martin Hellman que definia a criptografia assimétrica:
  - "New directions in Cryptography"
  - https://eclass.aueb.gr/modules/document/file.php/INF208/Diffie-Hellman76.pdf

- A finalidade do algoritmo é permitir que dois usuários compartilhem um valor secreto em segurança. Tal valor pode ser usado como chave para a criptografia subsequente das mensagens.

Diffie-Hellman (Ideia)



Retirado de: https://www.practicalnetworking.net/series/cryptography/diffie-hellman/

Diffie-Hellman (Ideia)

- A matemática por trás do algoritmo envolve aritmética modular e conceito de grupos cíclicos;

- Nos seguintes sites (ou na seção. 10.1 do livro texto) é possível encontrar uma explicação bem razoável sobre o funcionamento do algoritmo:
  - http://numaboa.com.br/criptografia/chaves/353-diffie-hellman?showall=&start=1
  - https://www.youtube.com/watch?v=NmM9HA2MQGI

- O importante aqui é que encontramos uma forma de **compartilhar um segredo** entre dois pares a partir de informações que foram trafegadas em claro!!

Diffie-Hellman (Ideia)

- Se *p* for um primo em torno de 600 dígitos (>=2048 bits) e *a* (segredo da Alice) e *b* (segredo do Bob) tenham em torno de 100 dígitos (> 224 bits), então até os melhores algoritmos conhecidos atualmente não poderiam encontrar *Private* dado apenas $G, P, G^{Private} \bmod P$ - *problema do logaritmo discreto*.

Princípios

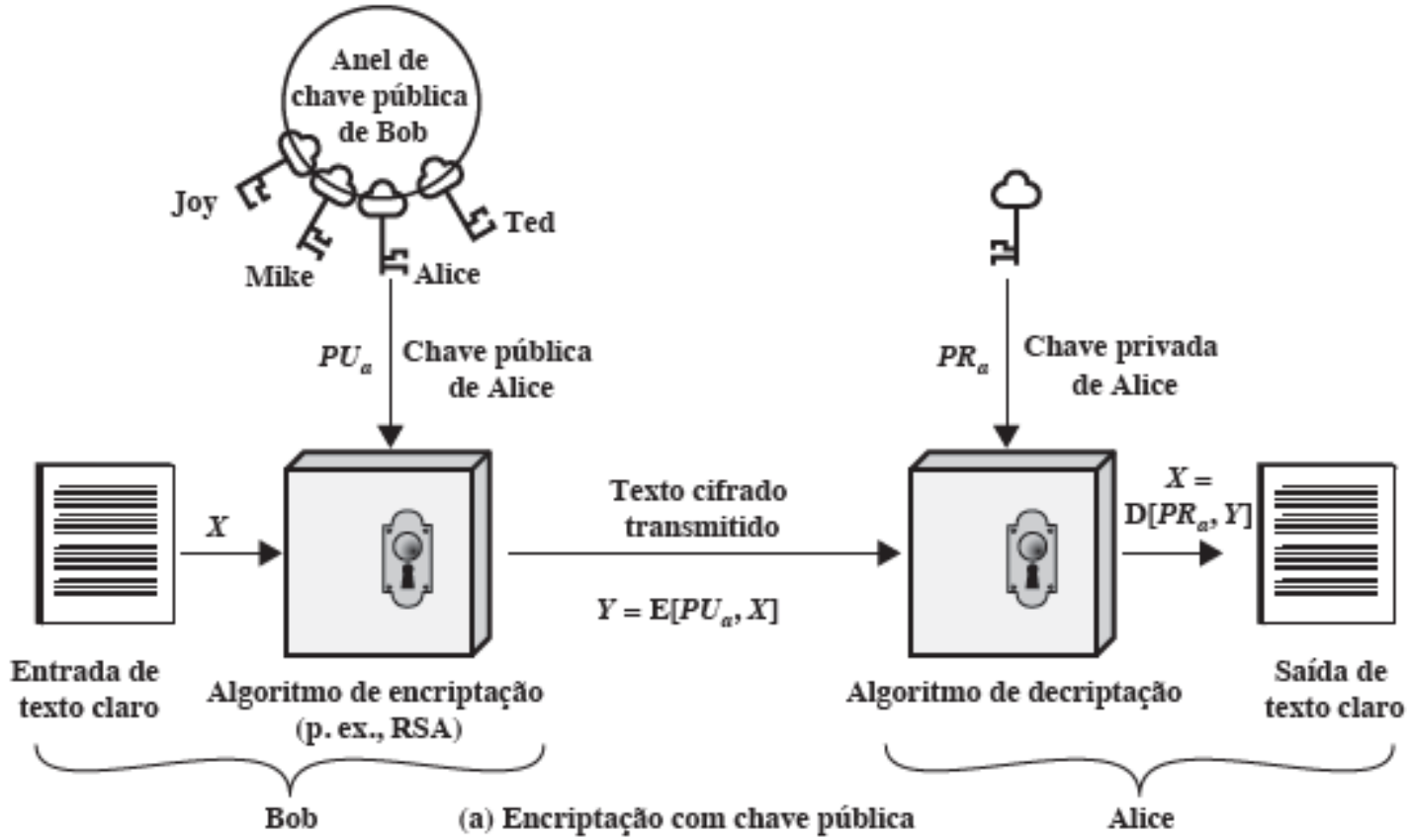
Segurança da Informação– GBC083

Duas chaves?!

Os algoritmos assimétricos contam com uma chave para *cifrar* e uma chave **diferente**, porém **relacionada**, para *decifrar*. Elas têm a seguinte característica:

"É computacionalmente inviável determinar a chave usada para decifrar dado apenas o conhecimento do algoritmo de criptografia e da chave para cifrar."

Elementos


Anel de chave pública de Bob
Joy
Ted
Mike
Alice
PU_a
Chave pública de Alice
PR_a
Chave privada de Alice
X
Texto cifrado transmitido
$Y = E[PU_a, X]$
$X = D[PR_a, Y]$
Entrada de texto claro
Algoritmo de encriptação (p. ex., RSA)
Algoritmo de decriptação
Saída de texto claro
Bob
(a) Encriptação com chave pública
Alice

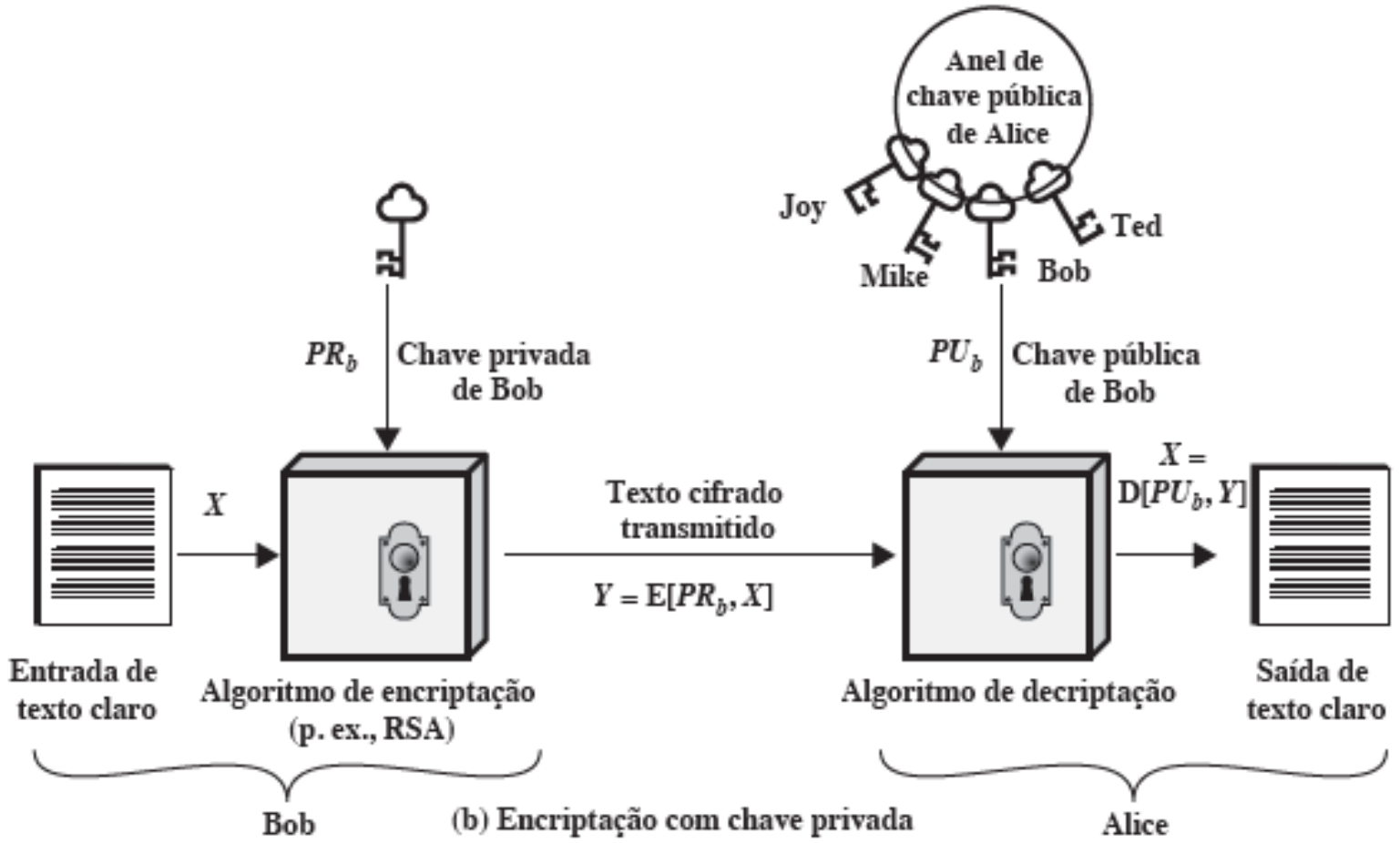
Princípios de criptografia assimétrica - Etapas

- Cada usuário gera um par de chaves;
- Cada usuário coloca uma das duas chaves em um registro público - chave pública. A outra chave permanece privada;
- Se Bob deseja enviar uma mensagem confidencial para Alice, Bob cifra a mensagem usando a chave pública de Alice;
- Quando Alice recebe a mensagem, ela decifra usando sua chave privada. Nenhuma outra pessoa pode decifrar a mensagem, pois somente Alice conhece a sua chave privada.

Outra característica...

"Qualquer uma das chaves pode ser usada para cifrar sendo a outra utilizada para decifrar."

Cifrar com a chave privada?



Cifrar com a chave privada?

- O que Bob ganha com isso?
- Quem poderá decifrar tal mensagem?
- Existe alguma garantia de confidencialidade?
- Discutiremos isso no decorrer da aula...

Requisitos

Segurança da Informação– GBC083

Requisitos

- Até agora vimos as características e como um sistema criptográfico assimétrico deveria funcionar;
- Quais são os requisitos, ou seja, como construir um algoritmo para suportar tais características?

Requisitos

1. É computacionalmente fácil* para uma entidade B gerar um par (PU_b PR_b);

2. É computacionalmente fácil* que um emissor A, conhecendo a chave pública e a mensagem a ser cifrada, *M*, gere o texto cifrado: $C = E(PU_b, M)$;

3. É computacionalmente fácil* que o receptor B decifre o texto cifrado C usando a sua chave privada;

* Fácil significa um problema que pode ser resolvido em tempo polinomial como função do tamanho da entrada.

Requisitos

4. É computacionalmente inviável* que um atacante, conhecendo a chave pública, PU_b, determine a chave privada PR_b;

5. É computacionalmente inviável* que um atacante, conhecendo a chave pública, PU_b e um texto cifrado C recupere a mensagem original M.

* Um problema é inviável se o esforço para solucioná-lo aumentar mais rapidamente do que o tempo polinomial em função do tamanho da entrada

Requisitos

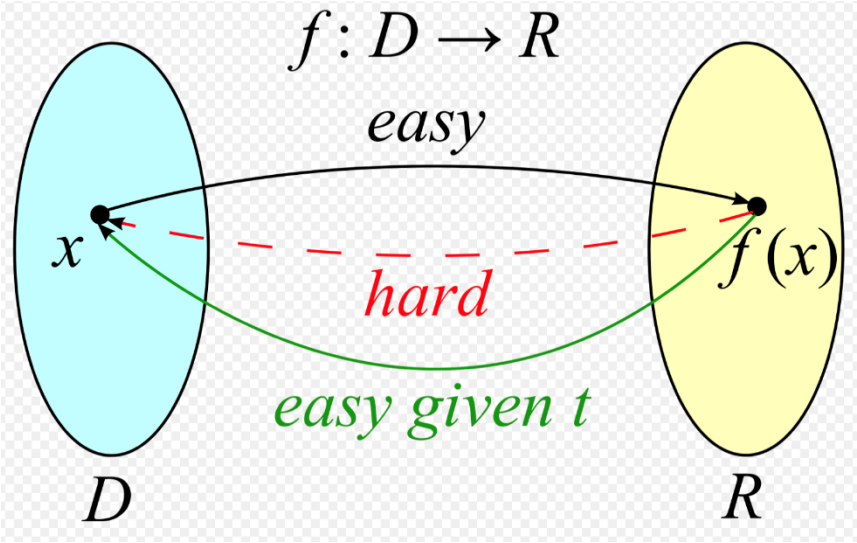
A ideia é construir uma função que tenha a seguinte propriedade:

- $C = E(PU_b, M)$ – fácil de calcular
- $M = D(PR_b, C)$ – fácil de calcular, se eu souber PR_b
  - Note que D é a inversa de E. A notação poderia ser E=f e $D = f^{-1}$

- $M = D(?, C)$ – inviável se eu não souber PR_b

Requisitos

- A função f deve ser uma *trapdoor function*;
- Fácil de se calcular em uma direção e inviável na outra, a menos que certa informação adicional seja conhecida.



Aplicações

Segurança da Informação– GBC083

Aplicações

- Os sistemas de chave pública são caracterizados pelo uso de um algoritmo criptográfico com duas chaves, uma mantida privada e uma disponível publicamente;

- Dependendo da aplicação, o emissor utiliza a sua própria chave privada ou a chave pública do receptor, ou ambas, para realizar algum tipo de função criptográfica.

Aplicações

Três aplicações para sistemas de criptografia assimétricos:

1. Cifrar/decifrar – confidencialidade;

2. Assinatura digital – não repúdio;

3. Troca de chaves – dois lados cooperam para trocar uma chave de sessão.
   - Vimos que o Diffie-Hellman proporciona isso. É possível estabelecer um modelo de troca de chaves usando somente as premissas de criptografia assimétrica?

Aplicações – assinatura digital

Veremos com mais cuidado esse conceito nas próximas aulas...

- A ideia consiste em uma entidade A usar a sua própria chave privada para cifrar uma mensagem M, gerando uma mensagem cifrada C.

- De acordo com os requisitos de criptografia assimétrica, a única chave que permite decifrar C seria a chave pública de A, ou seja, a chave que faz par com a chave usada para cifrar M.

Aplicações – assinatura digital

- Quem pode ler a mensagem cifrada C?

- O que isso garante?

Aplicações – assinatura digital

- Quem pode ler a mensagem cifrada C?

- O que isso garante?
  - Resposta: garante que a única pessoa que poderia ter enviado essa mensagem foi A, ou seja, A está ***assinando*** digitalmente a mensagem...

Aplicações – Troca de chaves

- Vamos supor que Alice quer trocar mensagens cifradas com Bob,

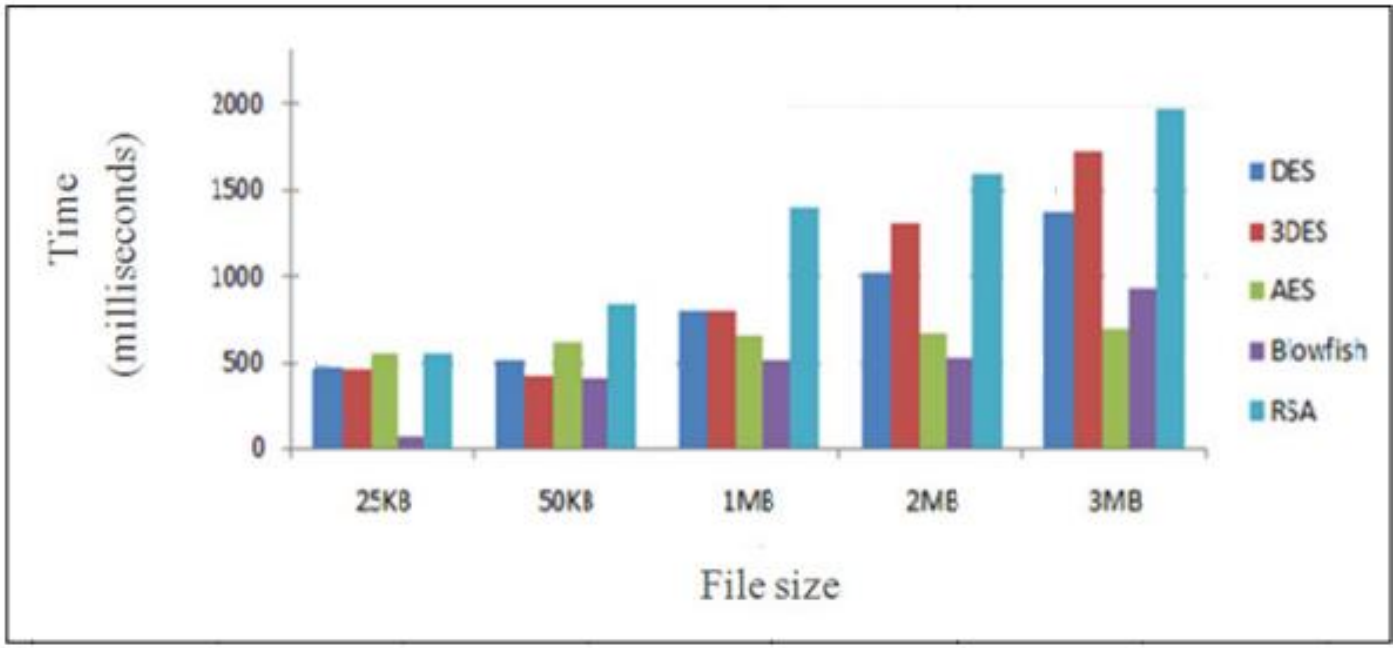
- Descrição dos passos:
  - 1) Alice gera uma chave "K", que será utilizada para cifrar todo o tráfego de mensagens entre eles;
  - 2) Alice obtêm a chave pública do destinatário, no caso Bob (Pub_Bob);
  - 3) Utilizando a chave pública de Bob, Alice envia a chave "K", cifrada com algum algoritmo de criptografia assimétrica;
  - 4) Do outro lado, Bob recebe a mensagem cifrada e utiliza a sua chave privada para decifrar a mensagem enviada por Alice. A mensagem contém a chave de suas trocas de mensagens, "K";
  - 5) Alice e Bob podem utilizar a chave "K" para cifrar as mensagens que serão trocadas entre eles.

Aplicações – Troca de chaves

Eu poderia combinar o modelo anterior com qual tipo de criptografia?

Algoritmos simétricos x assimétricos

- **Problema:** algoritmos assimétricos, por serem baseados em problemas matemáticos de difícil solução computacional, são mais lentos que os algoritmos simétricos!



- https://www.sciencedirect.com/science/article/pii/S1877050916001101

Criptografia – Modelo híbrido

- Criptografia simétrica:
  - Vantagem: boa performance computacional;
  - Desvantagem: troca de chaves;
- Criptografia assimétrica:
  - Vantagem: permite a troca segura de chaves;
  - Desvantagem: desempenho computacional ruim;
- Porque não unir os dois modelos?

Criptografia – Modelo híbrido

- Aplicação mais comum em criptografia:
  - 1) Geração da chave secreta "K"(sessão);
  - 2) A chave secreta "K" é cifrada utilizando um algoritmo assimétrico;
  - 3) Ambos, emissor e destino, compartilham a chave "K" sem prejudicar o canal;
  - 4) Envio seguro e eficiente de mensagens, utilizando algoritmos simétricos.

- Pontos fracos de ambos são reduzidos!

- TLS funciona exatamente dessa maneira – RSA formando o canal seguro e AES usado para o sigilo das informações;

Criptografia – Modelo híbrido

ALGORITMO	ENCRIPTAÇÃO/ DECRIPTAÇÃO	ASSINATURA DIGITAL	TROCA DE CHAVE
RSA	Sim	Sim	Sim
Curva elíptica	Sim	Sim	Sim
Diffie-Hellman	Não	Não	Sim
DSS	Não	Sim	Não

Criptoanálise

Segurança da Informação– GBC083

Criptoanálise

Algumas opções para o criptoanalista...

1. Força-bruta
   - Contra-medida – usar chaves grandes! Grande quanto? Depende do algoritmo...
   - Vimos que os sistemas de criptografia assimétricos dependem de algum tipo de função reversível.
   - Ou seja, o tamanho da chave precisa ser grande o suficiente para tornar o ataque de força bruta impraticável, mas pequeno para que a cifragem e a decifragem sejam viáveis computacionalmente.

Criptoanálise

2. Encontrar alguma maneira de calcular a chave privada, dado somente a chave pública.
   - Até o momento, não foi provado matematicamente que essa forma de ataque é **inviável** para determinado algoritmo de chave pública;
   - Assim, qualquer algoritmo, incluindo o RSA, é suspeito;
   - O controle é feito no tamanho da chave.

Criptoanálise

3. Ataque de mensagem provável.
   - Peculiar aos sistemas de chave pública;
   - Suponha que estou usando algum algoritmo de chave pública para enviar chaves do DES (56 bits);
   - O atacante poderia usar a chave pública do alvo e cifrar todas as possibilidades de chave do DES (56 bits);
   - Bastaria comparar o que está sendo enviado com o que ele calculou;
   - Acrescentar alguns bits aleatórios a mensagem que está sendo cifrada já ajudaria bastante na mitigação desse ataque.

Roteiro de estudos

1. Leitura da seção 9.1 do livro "Criptografia e segurança de redes. Princípios e práticas". William Stallings;
2. Estudo da vídeo-aula referente ao tópico 9;
3. Referências complementares:
   - https://medium.com/better-programming/an-introduction-to-public-key-cryptography-3ea0cf7bf4ba