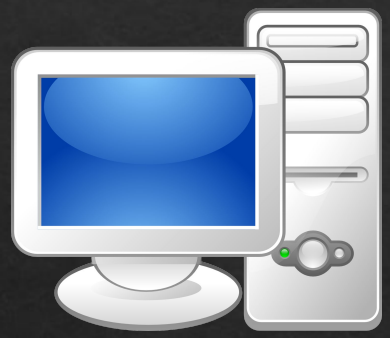
Algoritmo Diffie-Hellman

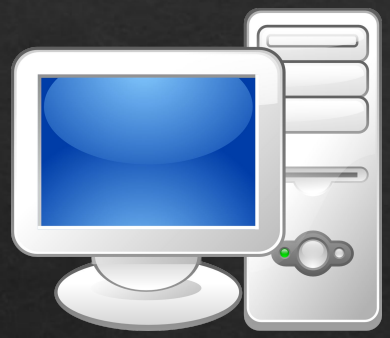
O que é criptografia?



Alice

Bob

O que é criptografia?



Alice

Chat?

Bob

Entrega dos postais sem troca de segredo

Alice

Bob

Entrega dos postais sem troca de segredo

Alice

Bob

Entrega dos postais sem troca de segredo

Alice

Bob

Entrega dos postais sem troca de segredo

Alice

Bob

Entrega dos postais sem troca de segredo

Alice

Bob

Entrega dos postais sem troca de segredo

Alice

Bob

Entrega dos postais sem troca de segredo

Alice

Bob

Entrega dos postais sem troca de segredo

Alice

Bob

Histórico

- Baseado na entrega segura de Carta dos Correios americanos;
  - Entrega em três passos;
- Criado em 1976;
- Foi a base dos negócios na internet;
- Ainda muito utilizado;
- Baseado em chave compartilhada;

Descrição

- Dois usuários concordam em valores para as variáveis N e G, sendo ambos números primos e N>G;
- Cada usuário escolhe um segredo S, número positivo que deve ser maior que 1;
- Cada usuário faz em separado a operação $P = G^S \bmod N$;
- Um usuário envia ao outro o resultado P; O outro usuário também envia o resultado P;
- Com o resultado o usuário que recebeu P faz a operação: $P^S \bmod N$
- Ambos terão uma chave compartilhada;

Passo 1

- Alice e Bob resolvem trocar mensagens.
- Escolha de G e N;
- G e N primos e N>G
- (Vamos usar números pequenos. Trata-se de uma demonstração.)

- G= 7
- N = 11

2- Escolha de um segredo e cálculo

- Alice e Bob escolheram G=7 e N =11

- Alice escolheu
- S = 6
- P= G^S mod N;
- P= 7^6 mod 11
- P=4

2- Escolha de um segredo e cálculo

- Alice e Bob escolheram G=7 e N =11

- Bob escolheu
- S = 3
- P= G^S mod N
- P= 7^3 mod 11
- P= 2

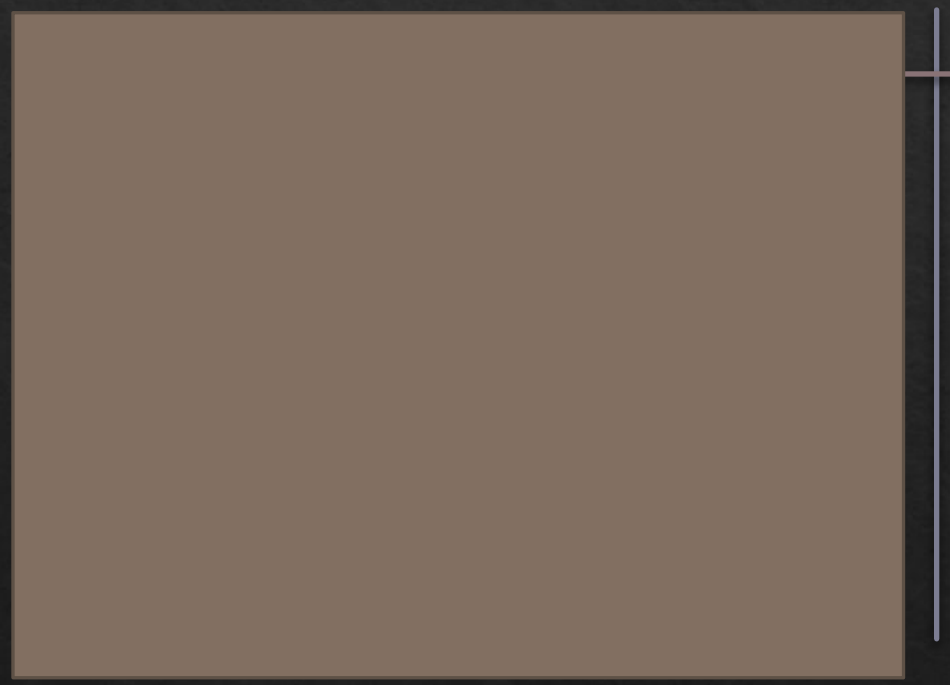
3- Troca de resultados e novo cálculo

- Alice tem P=4 e Bob tem P= 2

- Alice recebe P =2
- P = 2
- R= P^S mod N;
- R= 2^6 mod 11
- R=9

3- Troca de resultados e novo cálculo

- Alice tem P=4 e Bob tem P= 2



- Bob recebe P=4
- P = 4
- R= P^S mod N
- R= 4^3 mod 11
- R= 9

- Alice e Bob possuem uma chave compartilhada = 9

Características

- Usado para comunicação;
- Base do protocolo HTTPS;
- Não garante a identificação dos participantes;
- Um dos algoritmos mais importantes da História.