Universidade Federal do Ceará

Redes de Computadores

Disciplina: Segurança da Informação

Professor: David Sena

Alunos: Francisco Valdeir Maia Bandeira e Abimael Silas Barros

1- São chaves utilizadas para criptografar e descriptografar dados, cada uma com suas próprias características. A chave simétrica é uma chave única para criptografar e os dados, enquanto as chaves assimétricas são duas, uma chave pública e uma privada.

2-

Assimétrica: 2 chaves, pública e privada; chaves diferentes para criptografar e descriptografar; algoritmos mais complexos; mais lenta; mais segura.

Simétrica: Apenas 1 chave; mesma chave para criptografar e descriptografar; algoritmos mais simples; mais rápida; menos segura.

3-

Assimétrica: RSA e DSA(Algoritmo de Assinatura Digital)

Simétrica: RC4, AES e Máquina Enigma(Segunda Guerra Mundial)

4- Quando há a necessidade de se transmitir uma chave simétrica por um canal não seguro, a própria chave simétrica é cifrada com uma chave privada assimétrica e transmitida juntamente com a chave pública assimétrica para descriptografar a chave simétrica.

5 - KDC significa Centro Distribuidor de Chaves, o mesmo faz parte de um criptosistema destinado a reduzir riscos inerentes à troca de chaves. O KDC autentica o usuário através de um ticket, que será utilizado pra provar a identidade do usuário para os serviços disponíveis na rede. Ao receber uma requisição por ticket de uma máquina cliente o KDC cria um TGT (Ticket Granting Ticket), criptografa usando a senha secreta do usuário e o envia para o cliente que fez a solicitação. O KCD é responsável por gerar chaves para serem usadas por um pequeno período de tempo durante determinada conexão. Ele gera uma mensagem com 2 componentes: TGT e uma chave de sessão.

6 - O GPG é uma ferramenta de anonimidade na internet. Ele usa o método de chave pública e privada para assegurar a transferência de informações entre pares. Cada usuário cria uma chave pública e uma privada. A privada é guardada consigo e a pública é enviada aos pares com os quais se deseja realizar a troca de informações de forma segura por criptografia.

7- É um conjunto elaborado de práticas, técnicas e procedimentos que serve para suportar um sistema criptográfico baseado em certificados digitais. No Brasil é utilizado um sistema de certificação de raiz única em que todas as normas técnicas e operacionais são executadas pelo ITI, órgão do Governo responsável por esse controle.

8 - Por que eles não estão vinculados a um órgão capaz de assegurar sua identidade e autenticidade.