Criptografia Assimétrica

Jiyan Yari

Conceito

Conhecido como *algoritmos de chave pública e privada*, consiste no uso de duas chaves distintas.

Uma delas é usada para cifrar dados e a outra para decifrar, ou seja, o que uma chave faz, a outra desfaz.

Conceito

O problema da criptografia simétrica residia justamente no seu segredo, ou seja, a chave, pois o perigo no transporte dele poderia incorrer na sua captura e portanto a quebra da cifra.

Com esta preocupação Diffie e Hellman pensaram na ideia de dois cadeados, com duas chaves.

Conceito

Caso um emissor C queira enviar dados para um receptor F usando os correios, o procedimento poderia ser o seguinte:

- C requisita a F um cadeado;

- F vai em uma ferragem, compra um cadeado qualquer e o envia aberto para C, mantendo consigo a chave;

- C recebe pelos correios o cadeado aberto de F;

- C usa o cadeado para fechar a caixa e a envia para F.

Conceito

No entanto, para ser bem sucedido deve-se protegero o sigilo absoluto:

- o cadeado deve ser muito forte e uma vez fechado, só a chave pode abrí-lo;

- mesmo aberto, o cadeado não possui informações suficientes para que um chaveiro, mesmo habilidoso, consiga confeccionar uma nova chave para ele;

- o número de chaves possíveis inviabiliza que um chaveiro, mesmo com muito tempo, pudesse tentar cada uma delas.

Conceito

Diffie e Hellman foram os primeiros cientistas a descobrir uma função matemática de mão única e a usaram como base ao protocolo de troca de chaves.

Para que o assimétrico fosse possível, esta função de mão única precisa ser desfeita, mas apenas por quem conhece algum segredo em especial.

Conceito

No entanto, precisavam tornar a função de mão única reversível.

Tentaram, sem sucesso, chegar ao assimétrico, mas não conseguiram.

Porém apenas a idéia já foi importante o suficiente para que outros o fizessem.

Assim Ronald Rivest, Adir Shamir e Leonard Adlemann (RSA) conseguiram concretizar a idéia.

Conceito

No entanto, precisavam tornar a função de mão única reversível.

Tentaram, sem sucesso, chegar ao assimétrico, mas não conseguiram.

Porém apenas a idéia já foi importante o suficiente para que outros o fizessem.

Assim Ronald Rivest, Adir Shamir e Leonard Adlemann (RSA) conseguiram concretizar a idéia.

Conceito

As idéia da etapas essenciais consistiam em:

- cada usuário gera um par de chaves a ser usado para a criptografia e a descriptografia das mensagens;

- cada usuário coloca uma das duas chaves em um registro público ou outro arquivo acessível.

Esta chave foi chamada de pública por poder ser visualizada por outros sem acarretar perigo.

Conceito

A outra chave permanece privada, cada usuário mantém um conjunto de chaves públicas obtidas de outros usuários:

- se Bob deseja enviar uma mensagem confidencial para Alice, Bob criptografa a mensagem usando a chave pública de Alice;

- quando Alice recebe a mensagem, ela a descriptografa usando sua chave privada;

- nenhum outro destinatário pode descriptografar a mensagem, pois somente Alice conhece a sua chave privada.

Conceito

Com essa técnica, todos os participantes têm acesso às chaves públicas e as chaves privadas são geradas localmente não podendo ser distribuídas.

Desde que a chave privada de um usuário permaneça protegida e secreta, a comunicação que chega está protegida.

A qualquer momento pode-se alterar a chave privada e publicar a chave pública correspondente para substituir sua antiga chave pública

Conceito

Foi proposto um modelo de criptográfico chamado modelo de chave pública (Diffie e Hellman, 1978).

Neste modelo cada usuário possui um par de chaves (S, P) sendo S a sua chave particular, secreta, e P a sua chave pública.

Conceito

As chaves S e P são relacionadas matematicamente de tal forma que:

- se x denota um texto legível, e S() denota a aplicação da chave S, transforma x em S(x) =y então P(y) =x onde P() denota a aplicação da chave P, ou seja, S é a chave inversa da chave P onde, P(S(x)) =x;
- o cálculo do par de chaves (S, P) é computacionalmente fácil.
- é difícil o cálculo computacional para obter S a partir de P.
- os cálculos de P() e S() são computacionalmente fáceis para quem conhece as chaves.
- É computacionalmente difícil calcular S() sem conhecer a chave S.

Conceito

As condições da criptografia assimétrica levam ao fato de que:

- cada usuário calcula o seu par de chaves (S, P) no seu computador.

- a chave S é guardada de forma segura no seu computador.

- a chave P é distribuída a todos de forma pública.

Conceito

Alguns algoritmos assimétricos mais conhecidos e utilizados são:

- RSA;
- DSA;
- ElGamal;
- Diffie-Hellman;
- Curvas Elípticas.

RSA

Nome em homenagem aos seus inventores:

- Ron Rivest;
- Adi Shamir;
- e Len Adleman.

Foi criaram em 1977 no MIT e atualmente, é o algoritmo de chave pública mais amplamente utilizado, além de ser uma das mais poderosas formas de criptografia de chave pública conhecidas até o momento.

O RSA utiliza números primos.

RSA

A técnica do RSA consiste na facilidade de multiplicar dois números primos para obter um terceiro número, mas muito difícil de recuperar os dois primos a partir daquele terceiro número.

Exemplo:

Os fatores primos de 3.337 são 47 e 71.

Gerar a chave pública envolve multiplicar dois primos grandes; qualquer um pode fazer isto.

Derivar a chave privada a partir da chave pública envolve fatorar um grande número.

DSA

Criado pela NSA e patenteado pelo governo americano, o Digital Signature Algorithm (DSA), unicamente destinado a assinaturas digitais.

Foi proposto pelo NIST em agosto de 1991, para utilização no seu padrão Digital Signature Standard (DSS).

Adotado como padrão final em dezembro de 1994, trata de uma variação dos algoritmos de assinatura ElGamal e Schnorr.

ElGamal

O ElGamal é outro algoritmo de chave pública utilizado para gerenciamento de chaves. Sua matemática difere da utilizada no RSA, mas também é um sistema comutativo.

O algoritmo envolve a manipulação matemática de grandes quantidades numéricas. Sua segurança advém de algo denominado problema do logaritmo discreto.

Assim, o ElGamal obtém sua segurança da dificuldade de calcular logaritmos discretos em um corpo finito, o que lembra bastante o problema da fatoração.

Diffie-Hellman

Baseado no problema do logaritmo discreto, e o algoritmo de chave pública mais antigo ainda em uso.

O conceito de chave pública, aliás foi introduzido pelos autores deste algoritmo em 1976, porém ele não permite nem criptografia e nem assinatura digital.

O sistema foi projetado para permitir a dois indivíduos entrarem em um acordo ao compartilharem um segredo tal como uma chave, muito embora eles somente troquem mensagens em público.

Curvas Elípticas

Em 1985, Neal Koblitz e V. S. Miller propuseram de forma independente a utilização de curvas elípticas para sistemas criptográficos de chave pública.

Não é uma nova implementação, mas uma atualização de outras existentes (Diffie-Hellman e ElGamal) usando curvas elípticas.

Eles possuem o potencial de gerar chave pública mais segura e de menor tamanho, resolvendo o problema de chaves muito grandes.

Embora possuam o potencial de serem rápidos, são em geral mais demorados do que o RSA.

Sistemas Híbridos

Os algoritmos criptográficos podem ser combinados para a implementação dos três mecanismos criptográficos básicos:

- Criptografia (ciframento);

- Assinatura digital;

- e o hashing.

Sistemas Híbridos

Principais mecanismos dos protocolos criptográficos embutidos na arquitetura de segurança dos produtos destinados ao comércio eletrônico.

Provêm os serviços associados à criptografia que viabilizam o comércio eletrônico: disponibilidade, sigilo, controle de acesso, autenticidade, integridade e não-repúdio, usualmente apoiado por sistemas híbridos.

Sistemas Híbridos

Principais Sistemas Híbridos:

- IPSec;
- SSL e TLS;
- PGP;
- S/MIME;
- SET;
- X.509.

IPSec

Padrão de protocolos criptográficos desenvolvidos para o IPv6. Realiza também o tunelamento de IP sobre IP.

É composto de três mecanismos criptográficos: Authentication Header (define a função hashing para assinatura digital), Encapsulation Security Payload (define o algoritmo simétrico para ciframento) e ISAKMP (define o algoritmo assimétrico para gerência e troca de chaves de criptografia).

Criptografia e tunelamento são independentes, e permite Virtual Private Network (VPN) fim-a-fim.

SSL e TLS

Oferecem suporte de segurança criptográfica para os protocolos NTTP, HTTP, SMTP e Telnet.

Permitem utilizar diferentes algoritmos simétricos, message digest (hashing) e métodos de autenticação e gerência de chaves (assimétricos).

PGP

O Pretty Good Privacy (PGP), foi inventado por Phil Zimmermman em 1991, é um programa criptográfico famoso e bastante difundido na internet, destinado à criptografia de e-mail pessoal.

Algoritmos suportados: hashing: MD5, SHA-1 - simétricos:

- CAST-128;
- IDEA;
- e 3DES - assimétricos: RSA, Diffie-Hellman e DSS.

S/MIME

Secure Multipurpose Internet Mail Extensions (S/MIME) consiste em um esforço de consórcio de empresas, liderado pela SADSI e Microsoft, para adicionar segurança a mensagens eletrônicas no formato MIME.

Apesar do S/MIME e PGP serem ambos padrões para a internet, o S/MIME tem sua maior utilização no mercado corporativo, enquanto o PGP é utilizado em e-mail pessoal.

S/MIME

Secure Multipurpose Internet Mail Extensions (S/MIME) consiste em um esforço de consórcio de empresas, liderado pela SADSI e Microsoft, para adicionar segurança a mensagens eletrônicas no formato MIME.

Apesar do S/MIME e PGP serem ambos padrões para a internet, o S/MIME tem sua maior utilização no mercado corporativo, enquanto o PGP é utilizado em e-mail pessoal.

SET

Cojunto de padrões e protocolos, para realizar transações financeiras seguras, como as realizadas com cartão de crédito na internet.

Oferece um canal de comunicação seguro entre todos os envolvidos na transação.

Garante autenticidade X.509v3 e privacidade entre as partes.

X.509

Define o relacionamento entre as autoridades de certificação.

Faz parte das séries X.500 de recomendações para uma estrutura de diretório global, baseada em nomes distintos para localização.

Utilizado pelo S/MIME, IPSec, SSL/TLS e SET.

Baseado em criptografia com chave pública (RSA) e assinatura digital (com hashing).

Simétrica X Assimétrica

Diferenças básicas entre criptografia simétrica e assimétrica:

Criptografia simétrica ou chave privada	Criptografia assimétrica ou chave pública
Rápida	Lenta
Gerência e distribuição das chaves é complexa	Gerência e distribuição das chaves é simples
Não oferece assinatura digital	Oferece assinatura digital