Nomes: Cauã henrique; Luiz pengu pika pequena

Resumo Executivo

A necessidade de enviar comandos críticos (como desligar uma máquina industrial) de forma **confidencial e autêntica** exige a adoção de um modelo criptográfico robusto. A **Criptografia Assimétrica** (ou de Chave Pública) é a solução ideal, pois atende ao requisito de que "quem tranca não é a mesma chave que destranca". Ao utilizar um par de chaves (Pública e Privada), garantimos que apenas o destinatário legítimo (neste caso, o servidor ou o sensor) possa ler a mensagem, mesmo que o canal de comunicação seja interceptado.

mas você deve estar se perguntando, o que é criptografia.?

A criptografia é a prática de proteger informações por meio do uso de algoritmos codificados, hashes e assinaturas. As informações podem estar em repouso (como um arquivo em um disco rígido), em trânsito (como comunicação eletrônica trocada entre duas ou mais partes) ou em uso (durante a computação de dados). A criptografia tem quatro objetivos principais:

- **Confidencialidade**: disponibiliza as informações somente para usuários autorizados.
- **Integridade**: garante que as informações não tenham sido manipuladas.
- **Autenticação**: confirma a autenticidade das informações ou a identidade de um usuário.
- **Não repúdio**: impede que um usuário negue compromissos ou ações anteriores.

A criptografia usa vários algoritmos criptográficos de baixo nível para atingir um ou mais desses objetivos de segurança das informações. Essas ferramentas incluem algoritmos de encriptação, algoritmos de assinatura digital, algoritmos de hash e outras funções. Esta página descreverá alguns dos algoritmos criptográficos de baixo nível mais usados.

O que é uma chave criptográfica?

Uma chave é um grupo de caracteres aleatórios em uma ordem específica. Os protocolos de criptografia usam uma chave para alterar os dados de forma que sejam embaralhados e que ninguém sem a chave possa decodificar as informações.

💻 Solução Técnica Detalhada

A solução técnica baseia-se na compreensão e aplicação dos princípios da Criptografia Assimétrica, frequentemente combinada com a Simétrica em sistemas reais (modelo híbrido).

1. Analogia Didática: Chave Pública vs. Chave Privada

A Criptografia Assimétrica utiliza um **par de chaves** matematicamente ligadas, mas distintas:

- **Chave Pública (Cadeado Aberto Distribuído):**
    - É a chave que pode ser **compartilhada abertamente** (distribuída).
    - Sua função principal é **criptografar** dados para o proprietário da chave privada correspondente ou **verificar** assinaturas digitais criadas por ela.

    - *Analogia:* Imagine um **cadeado aberto** que você distribui a todos. Qualquer um pode usá-lo para trancar (criptografar) uma caixa de mensagem e enviá-la ao proprietário do cadeado.
- **Chave Privada (A Única Chave que Abre o Cadeado):**
    - É a chave que deve ser **mantida em absoluto segredo** pelo seu proprietário.
    - Sua função principal é **descriptografar** dados que foram criptografados com a Chave Pública correspondente ou **criar** assinaturas digitais.
    - *Analogia:* É a **única chave** que pode abrir o cadeado trancado pela Chave Pública. Apenas o destinatário pretendido tem esta chave para acessar a mensagem.

2. Diferenciação: Criptografia Simétrica vs. Assimétrica

O cenário de segurança exige a distinção entre dois modelos fundamentais de criptografia:

Característica	Criptografia Simétrica	Criptografia Assimétrica
Chaves Utilizadas	**Única Chave Secreta**	**Par de Chaves** (Pública e Privada)
Princípio	Mesma chave tranca e destranca	Uma chave tranca, a outra destranca
Velocidade	**Rápida** e eficiente	Mais **lenta** (maior custo computacional)
Segurança Principal	**Confidencialidade**	**Confidencialidade**, **Autenticidade** e **Não-Repúdio**
Uso Ideal	Criptografar **grandes volumes** de dados	**Troca segura de chaves** e **autenticação**

No contexto de IoT, geralmente se adota um **modelo híbrido**: a **criptografia assimétrica** (mais lenta e segura) é usada para a troca inicial de uma **chave simétrica** (mais rápida), que então é usada para criptografar o volume de dados da comunicação (comandos e telemetria).

3. Exemplos de Uso: HTTPS/TLS e SSH

Os protocolos de segurança que protegem a infraestrutura de comunicação em larga escala utilizam a criptografia de chave pública:

- **HTTPS/TLS (Transport Layer Security):**
    - É o protocolo que garante a segurança das transações na web.
    - A **criptografia assimétrica** é usada no *handshake* inicial para:

1. **Autenticar** o servidor (verificando seu Certificado Digital, que contém a Chave Pública).
2. **Trocar de forma segura** uma chave simétrica de sessão.

- A partir daí, a comunicação de dados é protegida pela **criptografia simétrica** (rápida).
- O HTTPS, não é nada mais que o protocolo de programa HTTP + SSL um protocolo que oferta uma camada de segurança para a criptografia de segurança.
- O HTTPS também pode ser uma junção do HTTP + o TLS ,ambos o SSL quanto o TLS apenas são protocolos que adicionam uma camada de segurança para que a criptografia ocorra;

Exemplo: Imagine que você está a navegar pela [INTERNET] e quer fazer [COMPRAS COMPLETAMENTE APROPRIADAS PARA SUA IDADE] nisso você clica em uma página que possui esses conteúdos, obviamente você não quer que seu HTTP seja visto por fora , se não haveria [VERGONHA ALHEIA EXTREMA] então sua busca é criptografada por SSL ou TLS, agora seus dados não podem ser acessados a não ser que eles tenham [A CHAVE MESTRA DO BALACOBACO{chave privada}] que está no seu computador, e você pode ver suas **—>[FOTOS VAZADAS DO PÉ DE LUIZPENGU CLIQUE AQUI]<--** sem que ninguém lhe incomode ou saiba;

- **SSH (Secure Shell):**
  - Usado para acesso e gerenciamento remoto seguro de servidores.
  - A **criptografia assimétrica** é amplamente utilizada para **autenticação**. Em vez de usar senhas, o usuário pode provar sua identidade (que é o dono da Chave Privada) ao servidor, que usa a Chave Pública correspondente para verificar a autenticidade, garantindo a integridade do comando enviado.

    Exemplo:

    Eu tenho um servidor na nuvem, ele roda Linux, ele hospeda um site. E se eu quiser instalar as atualizações nesse servidor? Se fosse um computador bem na minha frente, eu ia logar nele e abrir um shell/prompt de comando. Mas não tá na minha frente, é um servidor virtual localizado a 320 quilômetros de mim. Esse servidor tá rodando um programa SSH. Eu conecto nesse programa SSH usando um cliente SSH no meu laptop, e agora eu posso rodar os comandos pra instalar as atualizações do mesmo jeito que eu faria com o computador bem na minha frente; você pode usar isso como um VPN "meia boca".

Fontes: https://www.cloudflare.com/pt-br/, https://www.cloudflare.com/pt-br/learning/ssl/transport-layer-security-tls/,https://www-ssh-com.translate.goog/academy/ssh?_x_tr_sl=en&_x_tr_tl=pt&_x_tr_hl=pt&_x_tr_pto=tc, https://www.totvs.com/blog/gestao-para-assinatura-de-documentos/criptografia-simetrica-e-assimetrica/, https://www.reddit.com/r/learnprogramming/comments/1lr71qp/can_someone_please_explain_ssh_to_me/