**Criptografia híbrida** é uma abordagem que **combina criptografia simétrica e assimétrica** para aproveitar as vantagens de ambas, minimizando suas limitações.

**🔐 Definição**

**Criptografia híbrida** é uma técnica que utiliza **criptografia assimétrica para troca segura de chaves** e **criptografia simétrica para criptografar os dados em si**.

**⚙️ Como funciona o processo**

1. **O remetente gera uma chave simétrica aleatória** (ex: AES).
2. **Os dados são criptografados com essa chave simétrica** (porque é mais rápida e eficiente para grandes volumes).
3. **Essa chave simétrica é criptografada com a chave pública do destinatário** (usando criptografia assimétrica, como RSA ou ECC).
4. **Ambos os dados criptografados e a chave criptografada são enviados ao destinatário**.
5. O destinatário:
   * Usa sua **chave privada assimétrica para recuperar a chave simétrica**.
   * Usa a **chave simétrica para decifrar os dados**.

**✅ Vantagens**

| **Criptografia Simétrica** | **Criptografia Assimétrica** | **Criptografia Híbrida** |
| --- | --- | --- |
| Muito rápida | Troca de chaves segura | Une o melhor dos dois mundos |
| Difícil de escalar | Mais lenta | Escalável e eficiente |

**📦 Exemplo prático: TLS (HTTPS)**

Quando você acessa um site HTTPS:

1. O navegador e o servidor negociam uma **chave simétrica** usando **criptografia assimétrica** (por exemplo, com certificados X.509 e RSA).
2. Depois disso, os dados são transmitidos usando **criptografia simétrica (ex: AES)**.
3. Esse é um exemplo de **criptografia híbrida em ação**.

**🔑 Resumo**

| **Aspecto** | **Criptografia Híbrida** |
| --- | --- |
| Segurança da troca | Usa criptografia assimétrica |
| Rapidez na transmissão | Usa criptografia simétrica |
| Aplicações comuns | HTTPS/TLS, e-mails criptografados (PGP), VPNs |
|  |  |

A criptografia híbrida combina a criptografia simétrica e a assimétrica para oferecer segurança e eficiência. Ela usa criptografia assimétrica para trocar a chave simétrica de forma segura e, em seguida, usa essa chave simétrica para criptografar os dados reais, proporcionando velocidade e segurança.

Como funciona a criptografia híbrida:

1. **1. Troca de Chave Segura (Criptografia Assimétrica):**

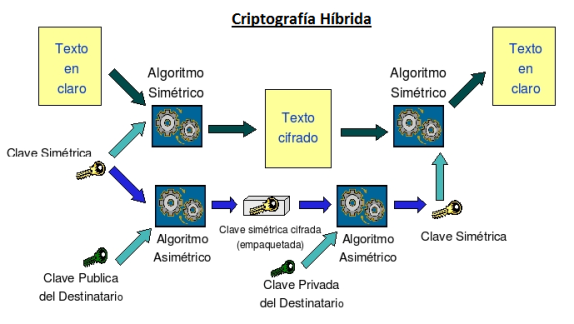
Um dos lados (remetente) gera uma chave aleatória e única para a comunicação, chamada chave de sessão. Essa chave é criptografada usando a chave pública do destinatário (criptografia assimétrica).

1. **2. Criptografia de Dados (Criptografia Simétrica):**

O remetente então usa essa chave de sessão (agora protegida) para criptografar a mensagem real usando um algoritmo simétrico (como AES), que é mais rápido do que a criptografia assimétrica para grandes quantidades de dados.

1. **3. Descriptografia:**

O destinatário usa sua chave privada para descriptografar a chave de sessão e, em seguida, usa essa chave de sessão para descriptografar a mensagem.



Vantagens da Criptografia Híbrida:

* **Segurança:**

Combina a segurança da criptografia assimétrica (troca segura de chaves) com a eficiência da criptografia simétrica (velocidade na criptografia de dados).

* **Eficiência:**

Permite criptografar grandes volumes de dados de forma rápida e segura usando a criptografia simétrica, após a chave de sessão ter sido trocada com segurança.

Exemplos de Aplicações:

* **HTTPS:**

Protocolo de comunicação segura usado em sites, onde a troca de chaves é feita com criptografia assimétrica e os dados são criptografados com criptografia simétrica.

* **Protocolos de Email Seguro (PGP, S/MIME):**

Utilizam criptografia híbrida para proteger o conteúdo de e-mails.

* **VPNs:**

Estabelecem túneis seguros entre clientes e servidores, utilizando criptografia híbrida para autenticação e troca de chaves, e criptografia simétrica para o fluxo de dados.

* **Assinaturas Digitais:**

A criptografia assimétrica é usada para criar uma assinatura digital, e a criptografia simétrica pode ser usada para proteger a integridade dos dados assinados.

Em resumo, a criptografia híbrida é uma abordagem estratégica que combina o melhor dos dois mundos (criptografia simétrica e assimétrica) para garantir segurança e eficiência em diversas aplicações de comunicação e proteção de dados.

**criptografia assimétrica e hibrida são a mesma coisa?**

Não, criptografia assimétrica e híbrida não são a mesma coisa. A criptografia assimétrica utiliza dois pares de chaves, uma pública e outra privada, para criptografar e descriptografar dados, enquanto a criptografia híbrida combina os dois métodos, usando a criptografia assimétrica para troca segura de chaves simétricas e a criptografia simétrica para criptografar os dados.

Criptografia Assimétrica:

* Usa um par de chaves: uma pública (compartilhada) e uma privada (secreta).
* A chave pública é usada para criptografar dados, e a chave privada correspondente é usada para descriptografar.
* Ideal para troca segura de chaves e autenticação, mas geralmente mais lenta que a criptografia simétrica para grandes volumes de dados.

Criptografia Híbrida:

* Combina criptografia simétrica e assimétrica.
* A criptografia assimétrica é usada para trocar uma chave simétrica de forma segura, por exemplo, usando a chave pública de um receptor para criptografar a chave simétrica.
* A chave simétrica criptografada é então enviada ao destinatário, que a descriptografa com sua chave privada.
* Finalmente, a criptografia simétrica é usada para criptografar os dados em si, aproveitando sua velocidade.
* Oferece a segurança da criptografia assimétrica na troca de chaves e a velocidade da criptografia simétrica para os dados.

Em resumo: A criptografia híbrida é uma abordagem que utiliza ambos os tipos de criptografia, enquanto a criptografia assimétrica é um dos métodos utilizados na abordagem híbrida.