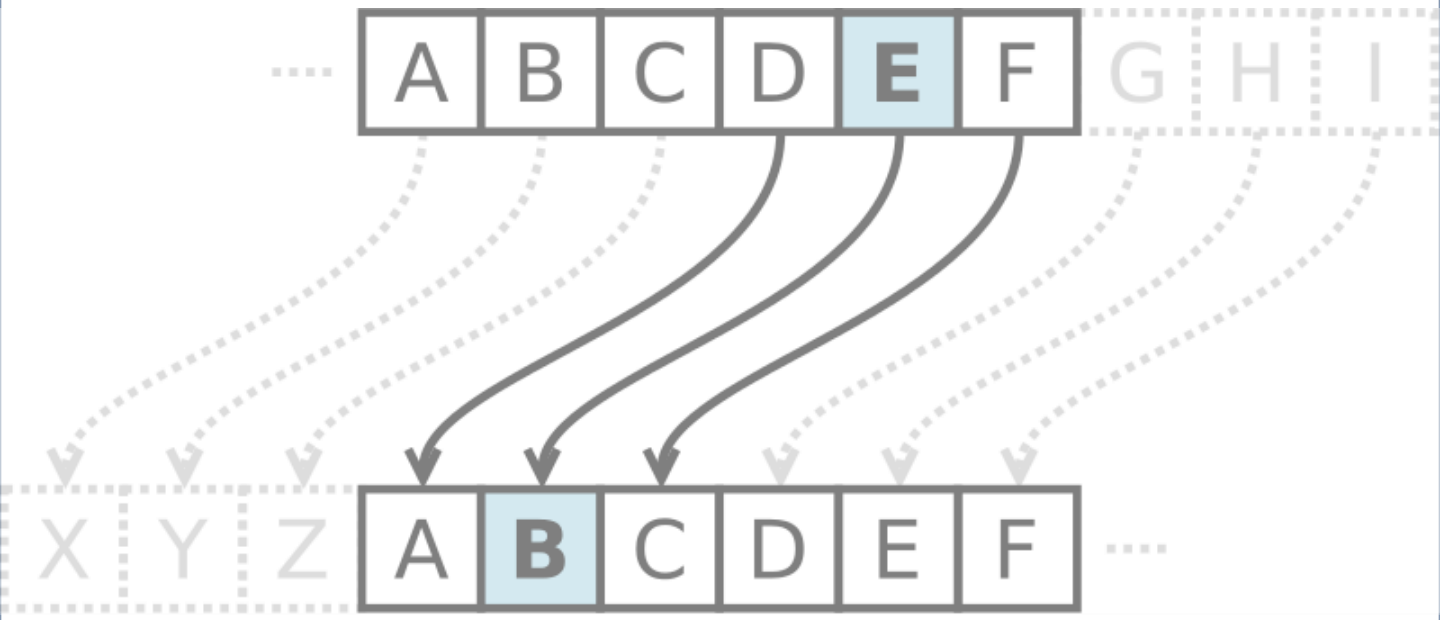
Breve introdução à Criptografia



compilado por

APSI

O que é a criptografia?

A criptografia é uma técnica de codificação de informação para proteger a sua confidencialidade e integridade durante a transmissão ou armazenamento.
Ao longo da história, a criptografia tem sido utilizada para salvaguardar mensagens, sejam elas militares, diplomáticas ou do foro pessoal.

compilado por

AP2SI

De que modo a criptografia protege a informação?

A criptografia implementa uma camada de segurança da informação, tornando-a ilegível para qualquer pessoa não autorizada.
Ao utilizar técnicas matemáticas avançadas, a criptografia protege as suas mensagens, senhas, dados pessoais e outra informação assegurando que apenas os destinatários pretendidos possam, compreendê-las, seja na internet ou fora dela.

compilado por

AP2SI

A cifra de César

Um dos primeiros exemplos registados de utilização de criptografia remonta à Roma Antiga, com o uso da "Cifra de César“, uma técnica simples de substituição de letras para proteger as mensagens militares durante as suas campanhas.
Como se pode ver na capa, com uma mudança de três posições, a letra A seria codificada como X, B como Y, e assim por diante.

compilado por

AP2SI

A importância da criptografia no mundo de hoje

A criptografia é o alicerce da confiança no mundo de hoje assegurando que as transações financeiras, trocas de mensagens, partilhas de dados e comunicações sejam realizadas de forma segura e protegida.

Desde o acesso ao seu banco às cidades inteligentes a cifra é o pilar da segurança e credibilidade na sociedade digital.

compilado por

AP2SI

A importância da criptografia para si

A criptografia é a sua defesa digital pessoal, garantindo a proteção da sua informação, de transações financeiras até às comunicações diárias.
Ao adotar a utilização de criptografia, fortalece a segurança da sua vida online, e assegura que apenas você e as pessoas autorizadas têm acesso aos dados que partilham.

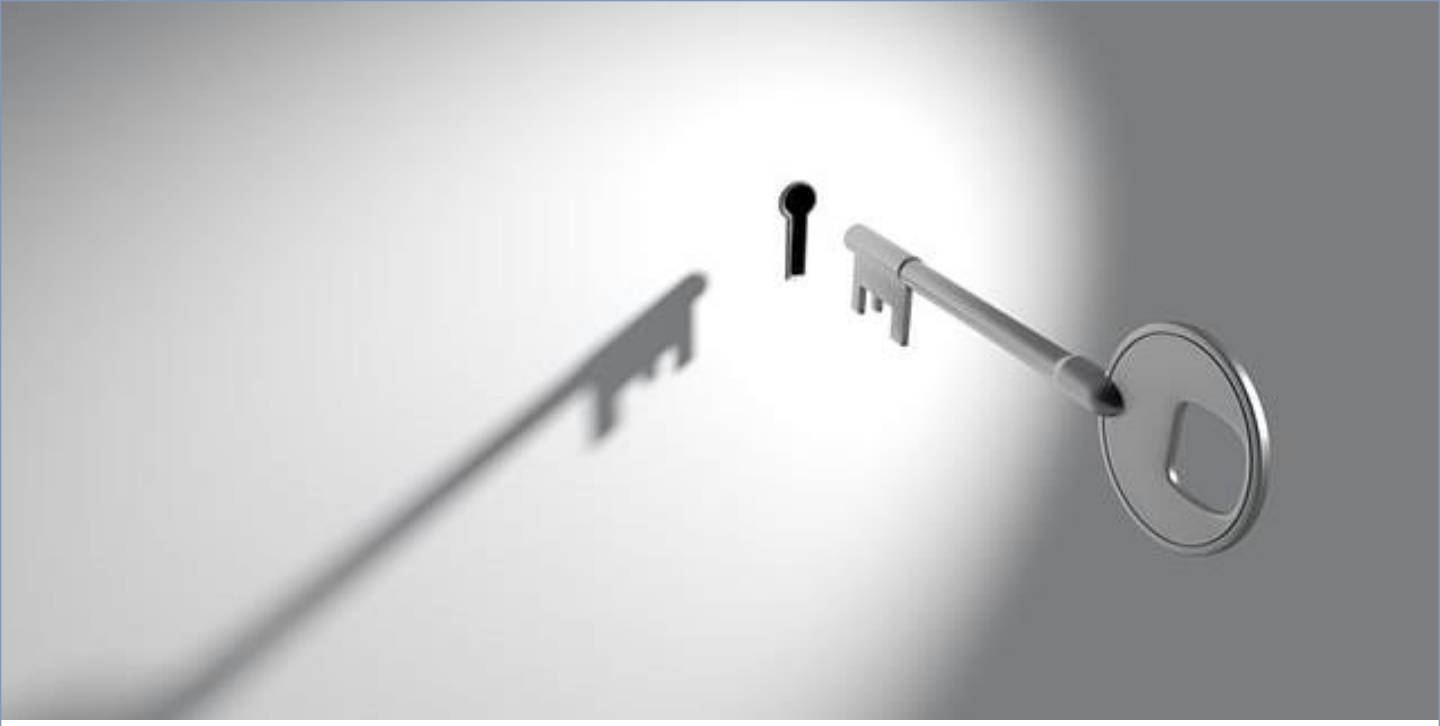
compilado por

AP2SI

Alguns conceitos de criptografia

compilado por

APSI



Chaves secretas

Uma chave secreta é um código ou sequência de caracteres utilizado para cifrar ou decifrar informação, fundamental para garantir a segurança das comunicações criptografadas.

O conceito de chave é aplicado tanto na criptografia simétrica como na assimétrica.

compilado por

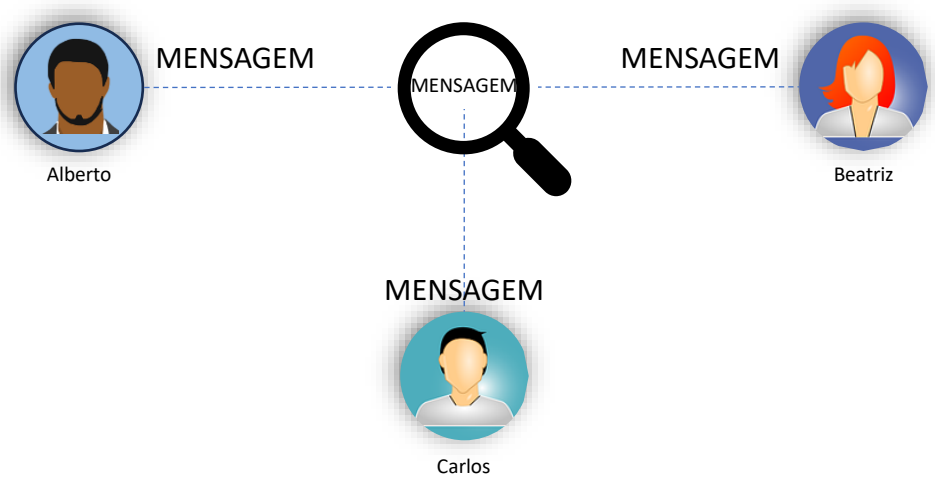
AP 2 SI

Chave Partilhada

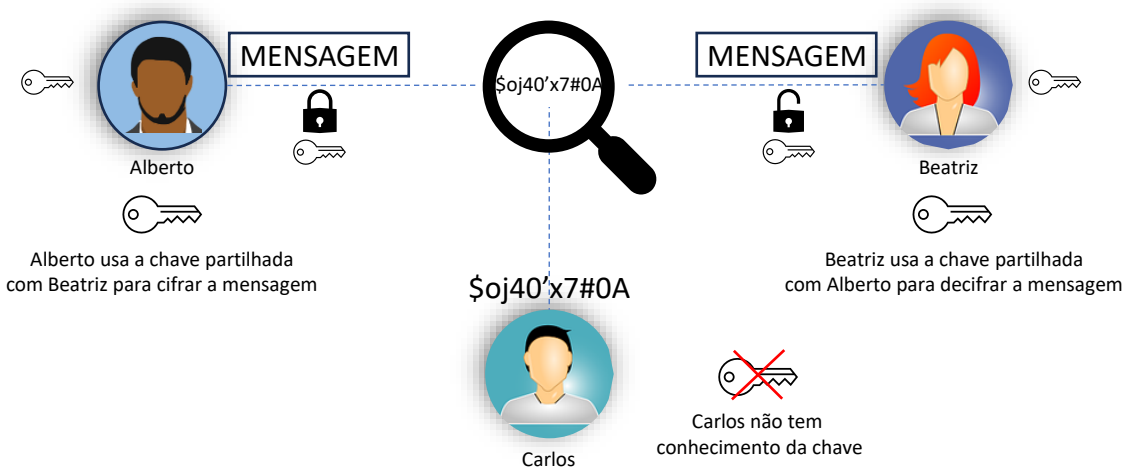
Na criptografia **simétrica** uma única chave é partilhada entre todos os participantes.

A mesma chave é utilizada tanto para cifrar como para decifrar os dados. A segurança está na proteção desta chave, pois qualquer pessoa que a conheça pode aceder à informação.

Troca de mensagens sem criptografia



Troca de mensagens com criptografia simétrica

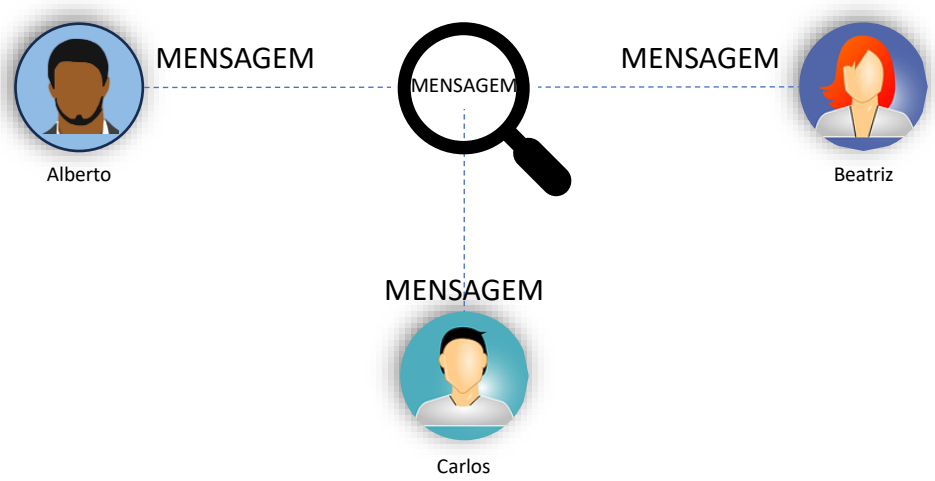


Chave Pública e Chave Privada

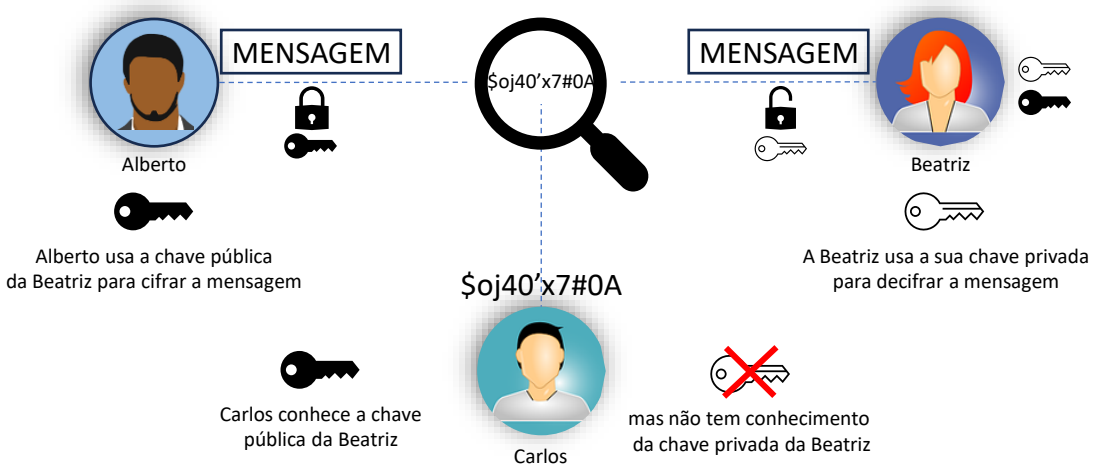
Na criptografia **assimétrica** cada utilizador tem um par de chaves: uma pública (partilhada abertamente) e outra privada (mantida em segredo).

A chave pública é utilizada por terceiros para cifrar as mensagens, e a chave privada é essencial para o próprio as decifrar. Este modelo também possibilita assinar as mensagens, assegurando a sua origem.

Troca de mensagens sem criptografia



Troca de mensagens com criptografia assimétrica



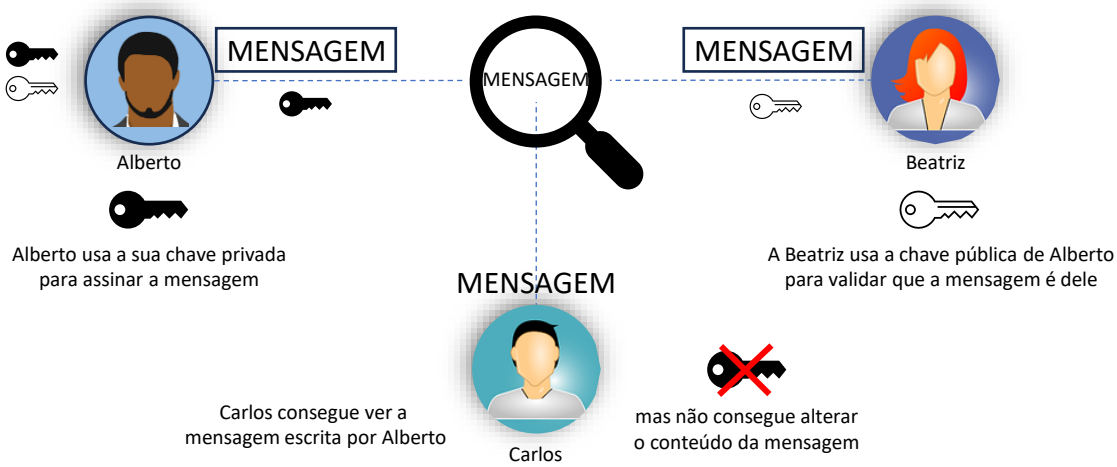
Assinaturas digitais

Assinaturas digitais são técnicas criptográficas que proporcionam autenticação, integridade e não repúdio em documentos eletrónicos ou transações online.
Funcionam de forma semelhante às assinaturas manuscritas em documentos físicos, mas são aplicadas digitalmente para garantir a autenticidade e a origem da informação.

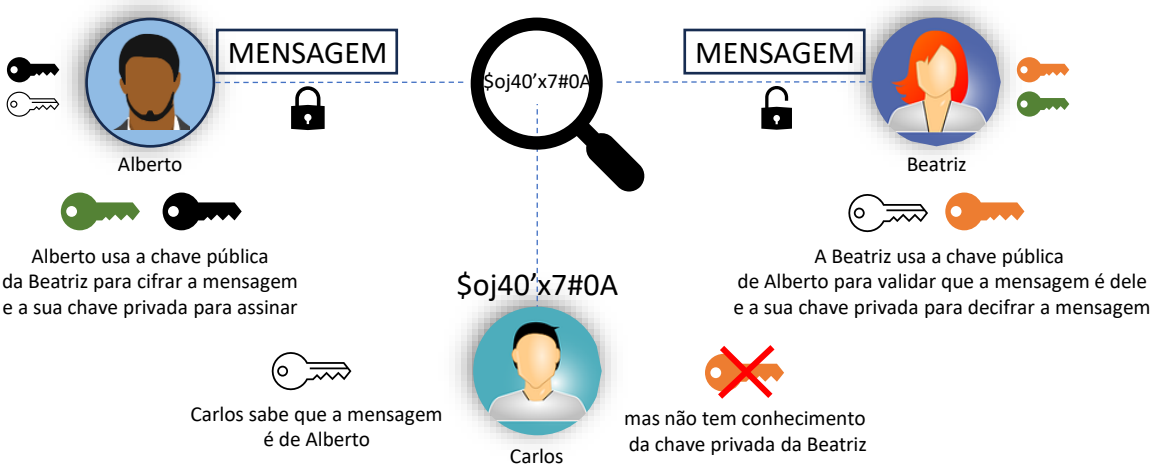
compilado por

AP2SI

Troca de mensagem com assinatura digital



Troca de mensagens com assinatura digital e criptografia assimétrica



Compilado por

Conheça melhor a AP2SI
em *https://ap2si.org*