SEGURANÇA EM ARMAZENAMENTO, TRATAMENTO E CONSUMO DE DADOS

PUC Minas Virtual

PUC Minas
Virtual

UNIDADE II – IMPLEMENTAÇÃO DA SEGURANÇA NOS DADOS

PUC Minas
Virtual

2.2 – SERVIÇOS E TÉCNICAS DE AUTENTICAÇÃO

PUC Minas
Virtual

2.2.3 – APLICAÇÃO DE TÉCNICAS DE CRIPTOGRAFIA

ASSINATURA DIGITAL

- É uma forma de mandar documentos e garantir ao destinatário que esse documento é autêntico. Adquire-se uma chave privada de uma autoridade certificadora onde pode-se assinar os documentos.
- O destinatário possui uma chave pública da mesma autoridade e consegue verificar a validade da assinatura e portanto a autenticidade do documento. É um recurso utilizado para eliminar o uso de assinatura física além de evitar a impressão de papéis desnecessariamente.

ENCRIPTAÇÃO DE EMAIL

- O envio de e-mails com **dados sensíveis** pode ser perigoso e facilmente interceptado por terceiros, podendo gerar prejuízos ao negócio.
- Existem meios de se encriptar os dados enviados, como, por exemplo, usando o **OpenPGP**.
- ***Pretty Good Privacy*** **(PGP)** é um software de criptografia utilizado em e-mails e arquivos confidenciais é open e combina os métodos de chave pública e privada.

ENCRIPTAÇÃO DE DADOS SENSÍVEIS

- Salvar dados sensíveis ao negócio (**como senhas ou financeiro**) deve ser feito de forma cuidadosa como as senhas estão armazenadas em um banco de dados, teremos que aplicar a **criptografia em repouso.**
- Mesmo que em ambientes corporativos haja a segregação entre o ambiente de desenvolvimento e produção, há risco de vazamento de dados se estes forem replicados de forma não controlada no ambiente.

ENCRIPTAÇÃO DE DADOS SENSÍVEIS

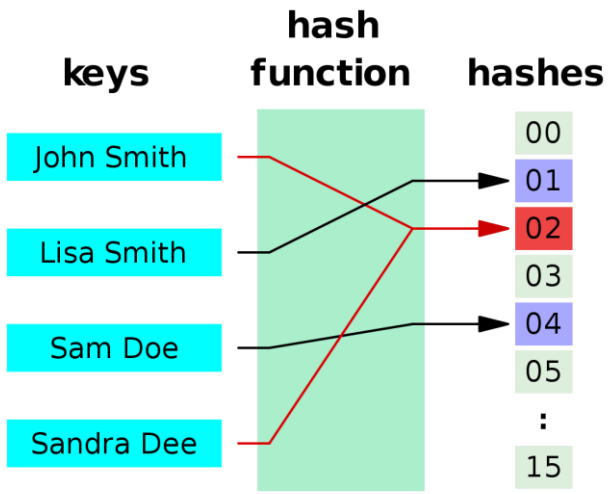
- Esta situação tem a ver com o vazamento de credenciais e afeta diretamente a reputação de um produto por exemplo, se houver vazamento da tabela de usuários e senhas de um sistema.
- Mesmo com o isolamento entre os ambientes administradores de sistemas e da infraestrutura podem vazar dados de usuários.

ENCRIPTAÇÃO DE DADOS SENSÍVEIS

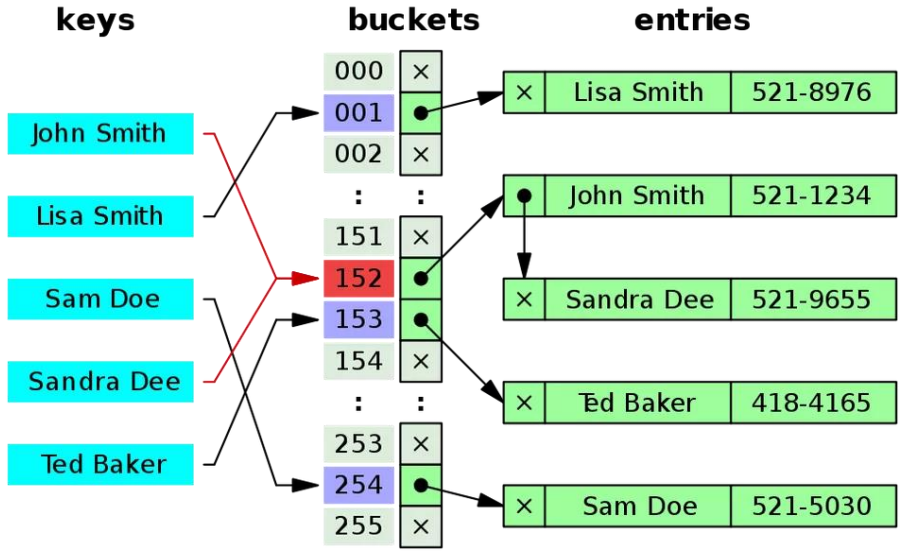
- Uma aplicação desta encriptação é a recomendação que antes de armazenar ou utilizar uma senha ela deve ser ***hasheada!***
- **HASH** é uma função que a partir de um texto original o transforma em outro texto envolvendo um cálculo matemático em um algoritmo do tipo ***one-way*** onde não é possível reverter o resultado.
- Outra vantagem é que ela converte com dados grandes e de tamanho variável para pequenos dados de tamanho fixo resumindo o dado.

ENCRIPTAÇÃO DE DADOS SENSÍVEIS

Fonte: LIMA, 2020



Fonte: STRINGFIXER, 2022



Fonte: STRINGFIXER, 2022

HTTPS/SSL:

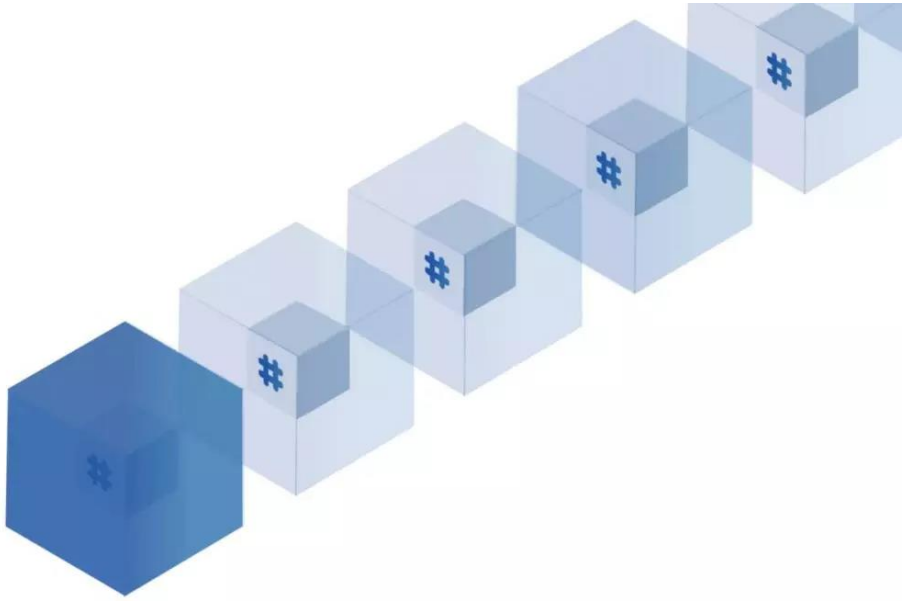
- Uma combinação de hash, criptografia e assinatura é usada no protocolo HTTPS, que está presente na maior parte dos sites na web hoje em dia sugiro que se não houver a aplicação desta técnica nos sites que você está consumindo que você mude de serviço.
- Isso garante que o site que você está acessando realmente **é de quem você espera que seja** e que as informações trafegadas estão seguras tais como senha, dados pessoais, etc.
- Nesta situação aplicamos o conceito de criptografia em trânsito.

BLOCKCHAIN:

- É uma tecnologia moderna onde se aplicam os princípios de criptografia para armazenar os dados e verificar sua autenticidade simultaneamente, além de outros usos.
- É composta por uma sequência de blocos que armazenam informação criptografada sobre todas as transações feitas.

BLOCKCHAIN:

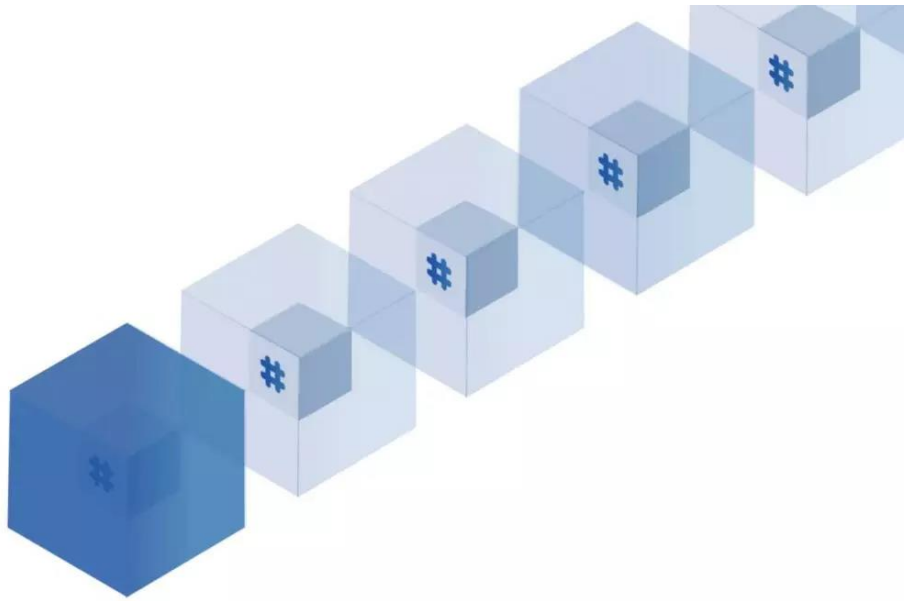
- Cada bloco possui um *Trasaction ID* **(TXID)** que é uma chave pública, transformados em um novo *hash* a cada iteração, que representa cada troca feita.



Fonte: LIMA, 2020

BLOCKCHAIN:

- Quando um novo bloco é criado, esse bloco terá informação sobre uma série de **novas transações** e ainda a ***hash* do bloco anterior**, criando assim uma **nova *hash***, única, mas "geneticamente" ligada ao bloco anterior.



Fonte: LIMA, 2020

REFERENCIAS BIBLIOGRÁFICAS

MACÊDO, Diego**.** Chaves Simétricas e Assimétricas, 2011. Disponível em: <https://www.diegomacedo.com.br/chaves-simetricas-assimetricas/>. Acesso em: 20 Set. 2022.

LIMA, Marcela**.** Hashing – O Que É e Como Funciona nas Criptomoedas?, 2020. Disponível em: < https://criptofy.com/hashing-criptomoedas/ >. Acesso em 28 Set. 2022.

STRINGFIXER, 2022. Função Hash. Disponível em:<https://stringfixer.com/pt/Hash_sum>.Acesso em: 27 Set. 2022.


PUC Minas
Virtual