Prof. esp. Thalles Canela

- **Graduado:** Sistemas de Informação - Wyden Facimp
- **Pós-graduado:** Segurança em redes de computadores - Wyden Facimp

- **Professor (contratado):**
- **Pós-graduação:** Segurança em redes de computadores - Wyden Facimp
- **Professor (Efetivado):**
- **Graduação:** Todo núcleo de T.I. - Wyden Facimp
- **Tech Lead na Motoca Systems**

Redes sociais:

- **Linkedin:** https://www.linkedin.com/in/thalles-canela/
- **YouTube:** https://www.youtube.com/aXR6CyberSecurity
- **Facebook:** https://www.facebook.com/axr6PenTest
- **Instagram:** https://www.instagram.com/thalles_canela
- **Github:** https://github.com/ThallesCanela
- **Github:** https://github.com/aXR6
- **Twitter:** https://twitter.com/Axr6S

Por que a criptografia é tão importante atualmente?

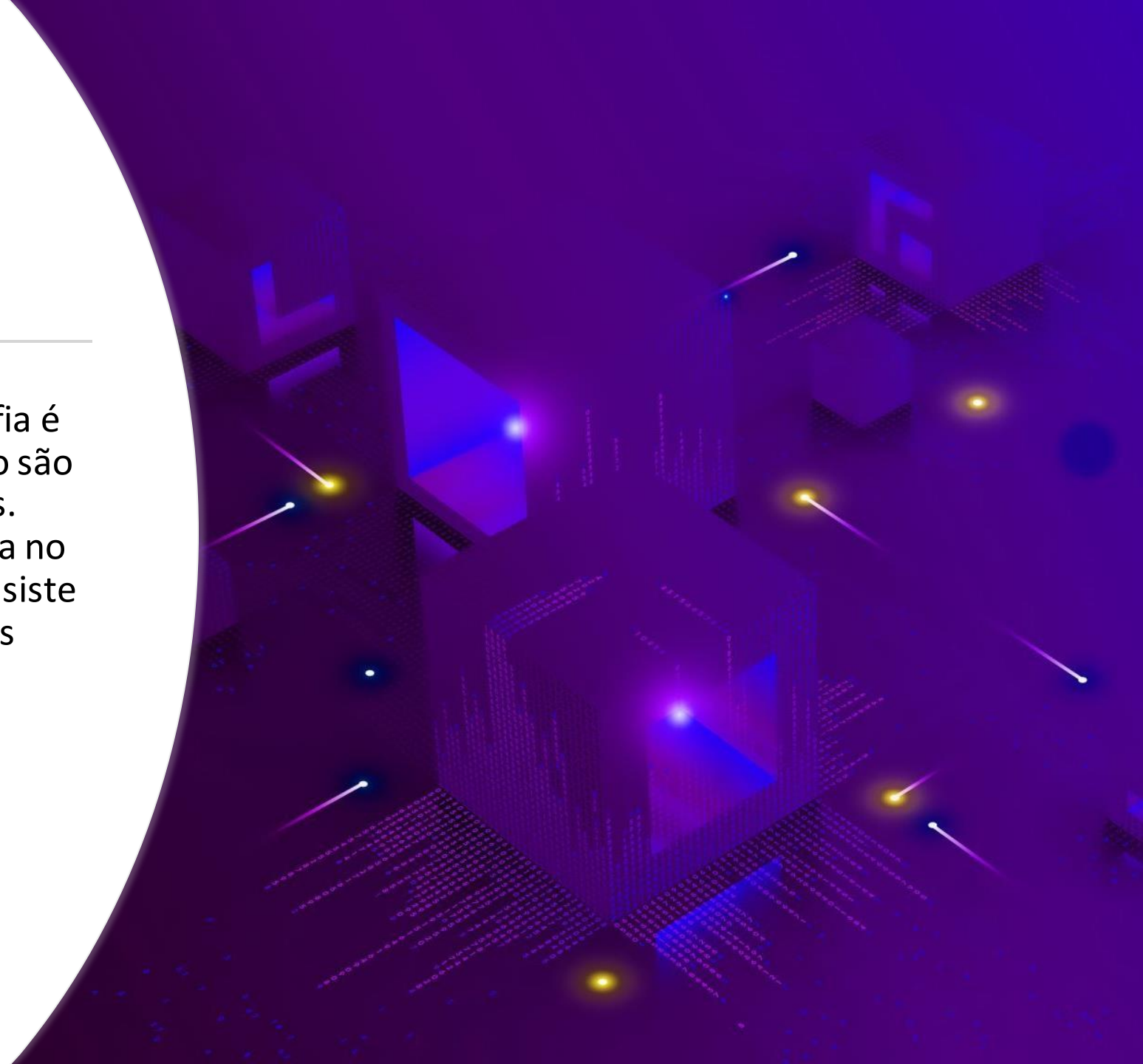
- A criptografia é uma das primeiras barreiras para impedir que um cibercriminoso (como hackers) tenha acesso aos seus dados durante o envio de mensagens, de forma de evitar a interceptação de informações.

Quais são os principais tipos de criptografia?

- Escolher o tipo de criptografia ideal para o seu negócio é fundamental para não incorrer em erros e deixar os seus dados desprotegidos, podendo ser acessados por outros usuários maliciosos. Para isso, neste texto, vamos explicar sobre os principais tipos de criptografia existentes no momento.

Tipos de criptografia

- O modo de funcionamento da criptografia é simples: os dados legíveis de um arquivo são codificados para que pareçam aleatórios. Trata-se de um mecanismo que se baseia no uso de uma chave criptográfica, que consiste em um conjunto de valores matemáticos disponibilizado para o remetente e o destinatário.



Chave simétrica

- A chave simétrica é o modelo mais comum e simples. Nela, uma mesma chave é utilizada tanto pelo emissor como pelo receptor da mensagem — ou seja, ela é usada tanto para a codificação como para a descodificação dos dados.

- Esse tipo de criptografia foi responsável por lançar as bases para outros modelos, como o DES e o IDEA.

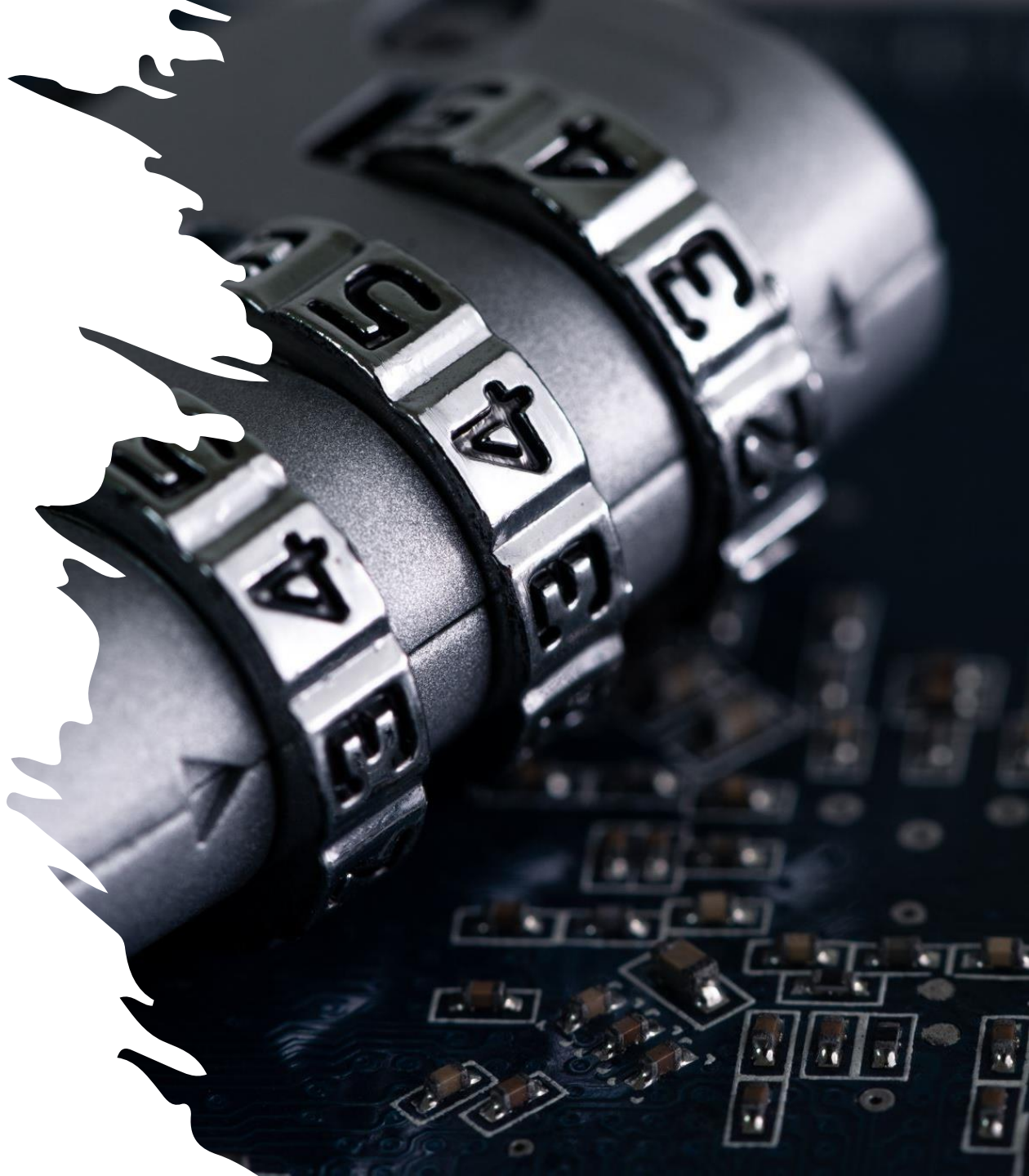
Chave assimétrica

- Também conhecida como “chave pública”, trabalha tanto no modo privado quanto no público. No primeiro, a chave é secreta. Já no modelo público, o usuário deverá criar uma chave de codificação e encaminhá-la para o receptor, para que possa ter acesso ao conteúdo.

DES (Data Encryption Standard)

- Esse é um dos modelos mais básicos, tendo sido um dos primeiros a ser criados (pela IBM, em 1977) e implementados. Consequentemente, é um dos mais difundidos mundialmente, pois fornece uma proteção básica de apenas cerca de 56 bits, oferecendo até 72 quatrilhões de combinações.

- Esse método pode ser decifrado por meio de uma técnica chamada “força bruta”. Nesse caso, um programa testa, constantemente, todas as possibilidades de chave, de forma automatizada e por horas seguidas. Como é um sistema de proteção básica, oferece uma segurança reduzida para o usuário.

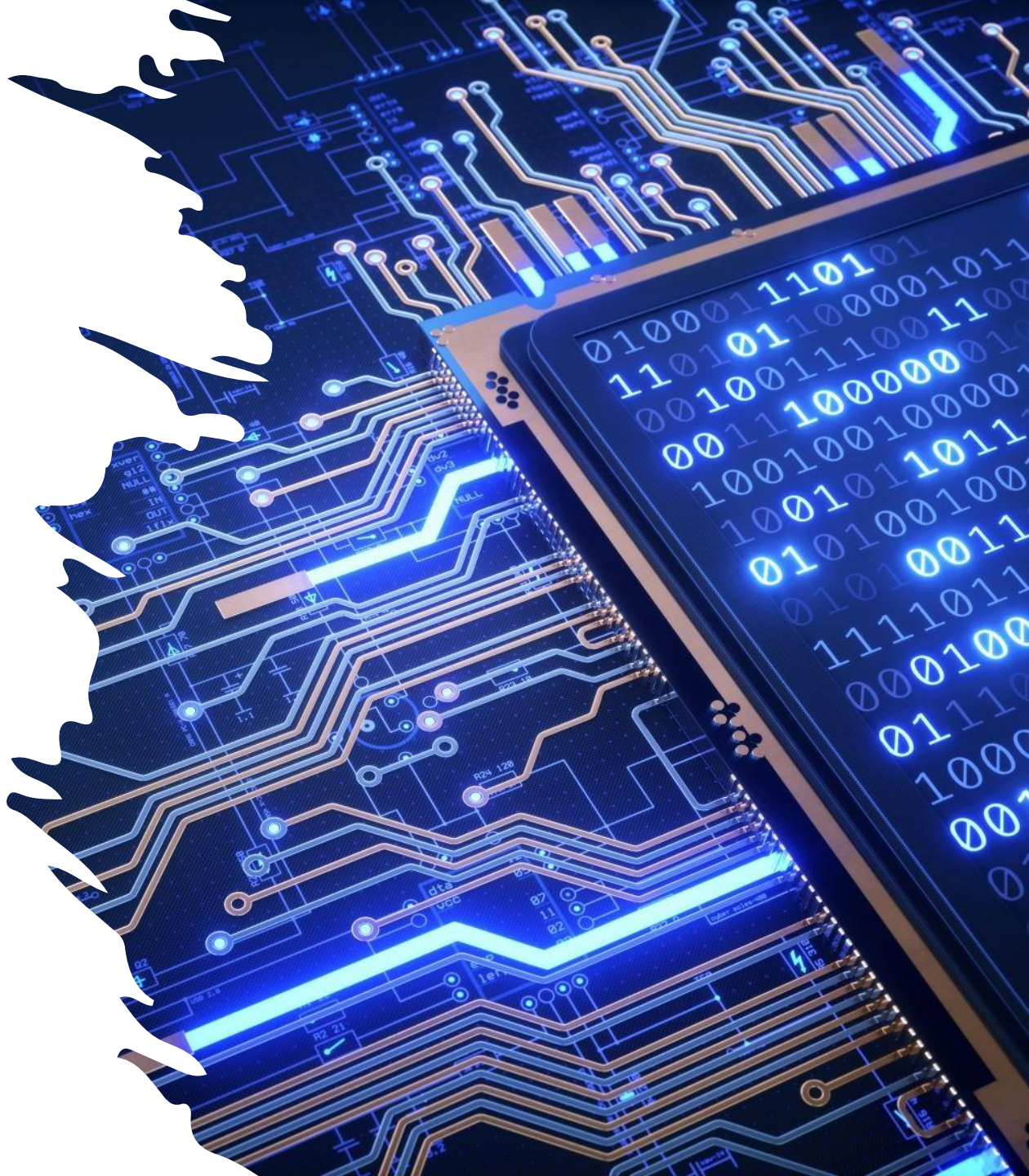


IDEA (International Data Encryption Algorithm)

- Criada em 1991, essa é uma chave simétrica que opera em blocos de informações de 64 bits e utiliza chaves de 128 bits. Ela atua de forma diferenciada, fazendo uma espécie de confusão para cifrar o texto, protegendo as informações e impedindo o realinhamento para a sua leitura de forma correta. Sua estrutura é bastante semelhante à do DES.

SAFER (Secure and Faster Ecryption Routine)

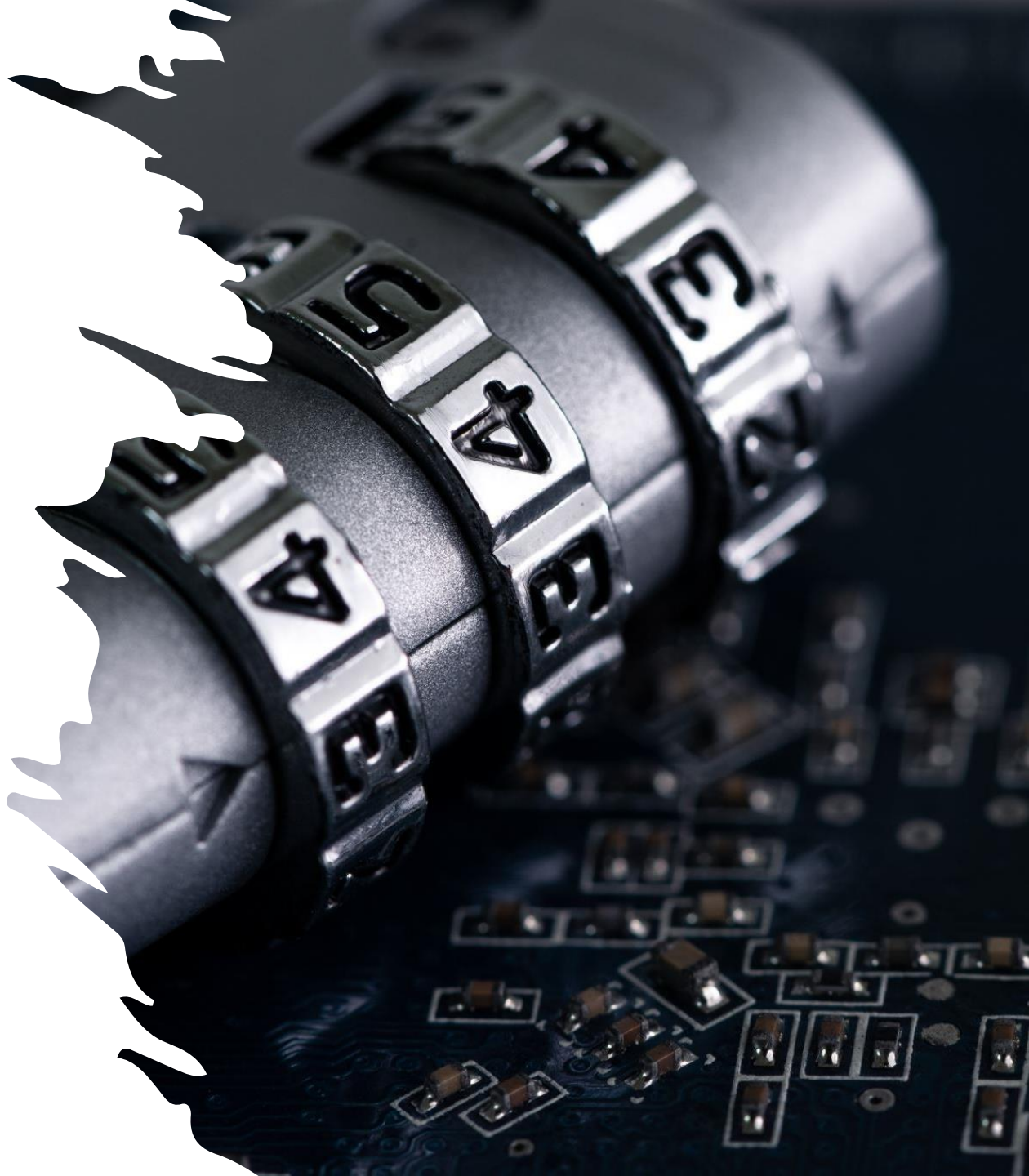
- Nesse modelo, a criptografia é feita em blocos de 64 bits. Não raro, o usuário poderá encontrá-la pelo nome de SAFER SK-64. Porém, é uma criptografia na qual muitos especialistas encontraram diversas fragilidades, fazendo com que fossem desenvolvidas novas opções mais complexas, como o SK-40 e o SK-128 bits.



SSL (Secure Sockets Layer)

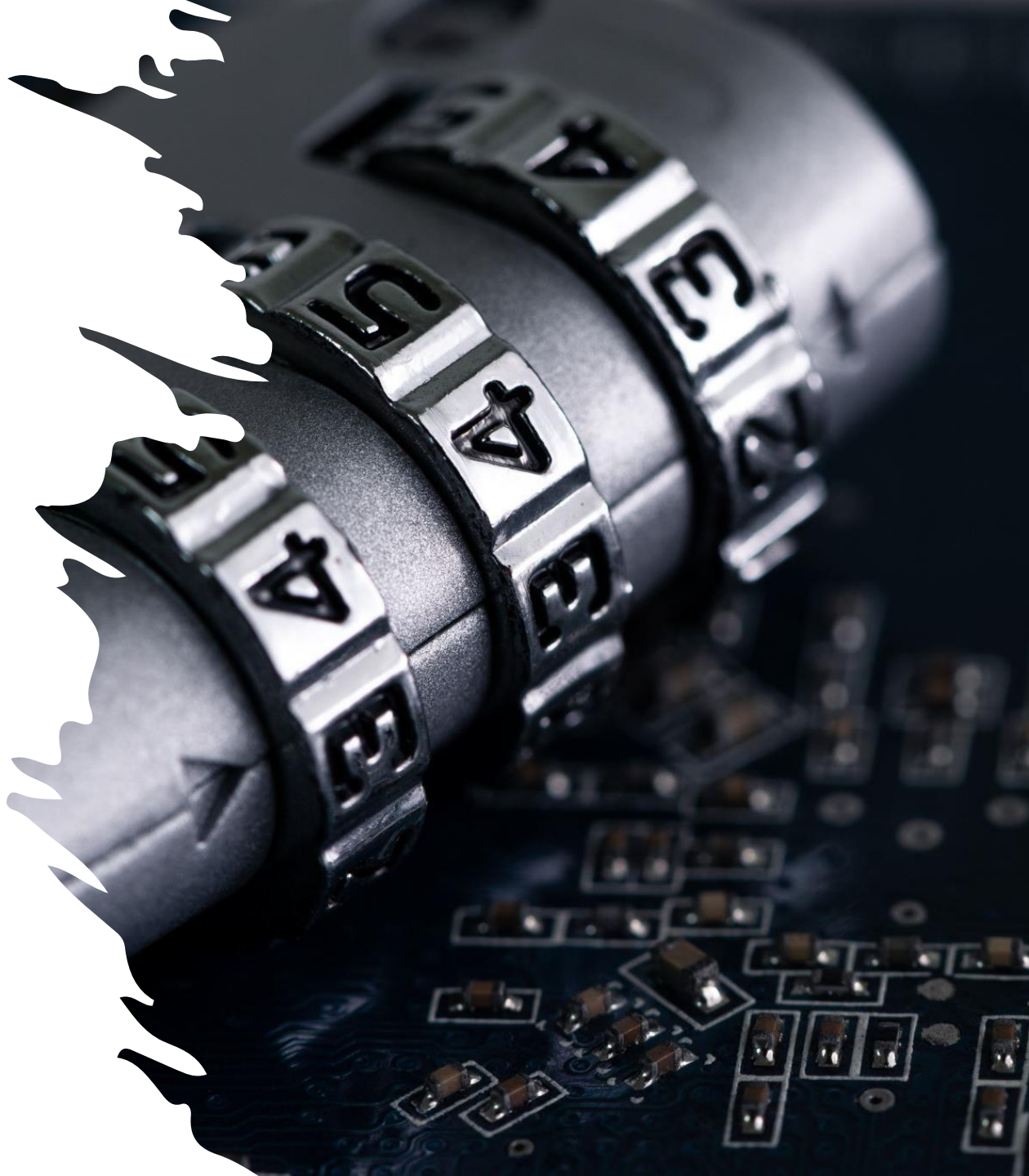
- A criptografia Secure Socket Layer (SSL), que em português significa Camada de Soquete Seguro, mantém os canais de comunicação criptografados durante a transferência de dados.

- O SSL funciona a partir de uma chave pública e outra privada, possibilitando a troca segura de informações entre aplicativos e servidor. Para enviar a chave pública, o sistema verifica se o certificado enviado é confiável, válido e se relaciona com o site que o enviou. A mensagem criptografada com chave pública só é decifrada com a inserção da chave privada.



AES (Advanced Encryption Standard)

- É um dos algoritmos de criptografia mais seguros da atualidade, sendo utilizado até mesmo pelo Governo dos Estados Unidos e, também, por diversas organizações de segurança. Sua criptografia é feita em blocos de 128 bits, mas as chaves podem ser aplicadas também em 192 e 256 bits, tornando essa chave extremamente difícil de ser quebrada em ataques convencionais de cibercriminosos.



Qual é a importância de utilizar a criptografia em todos os dispositivos?

- Um erro comum dos gestores é aplicar a criptografia apenas nas comunicações em máquinas físicas (notebooks e desktops), ignorando o uso desse recurso em dispositivos móveis (smartphones, tablets e wearables). Cada vez mais, as comunicações e os envios de informações e dados são utilizados por meio dessa segunda modalidade, e os cibercriminosos, conscientes disso, atacam justamente a vulnerabilidade desses sistemas.

Como escolher o melhor tipo de criptografia para a empresa?

- A escolha deve ser feita de acordo com o nível de sigilo dos dados do seu negócio. Empresas que trabalham com um grande número de informações delicadas (como grandes bancos de dados de clientes e usuários, ou empresas relacionadas com a área de segurança) necessitam de proteções extras, implementando não só a criptografia, mas também outros protocolos ligados a cybersecurity.