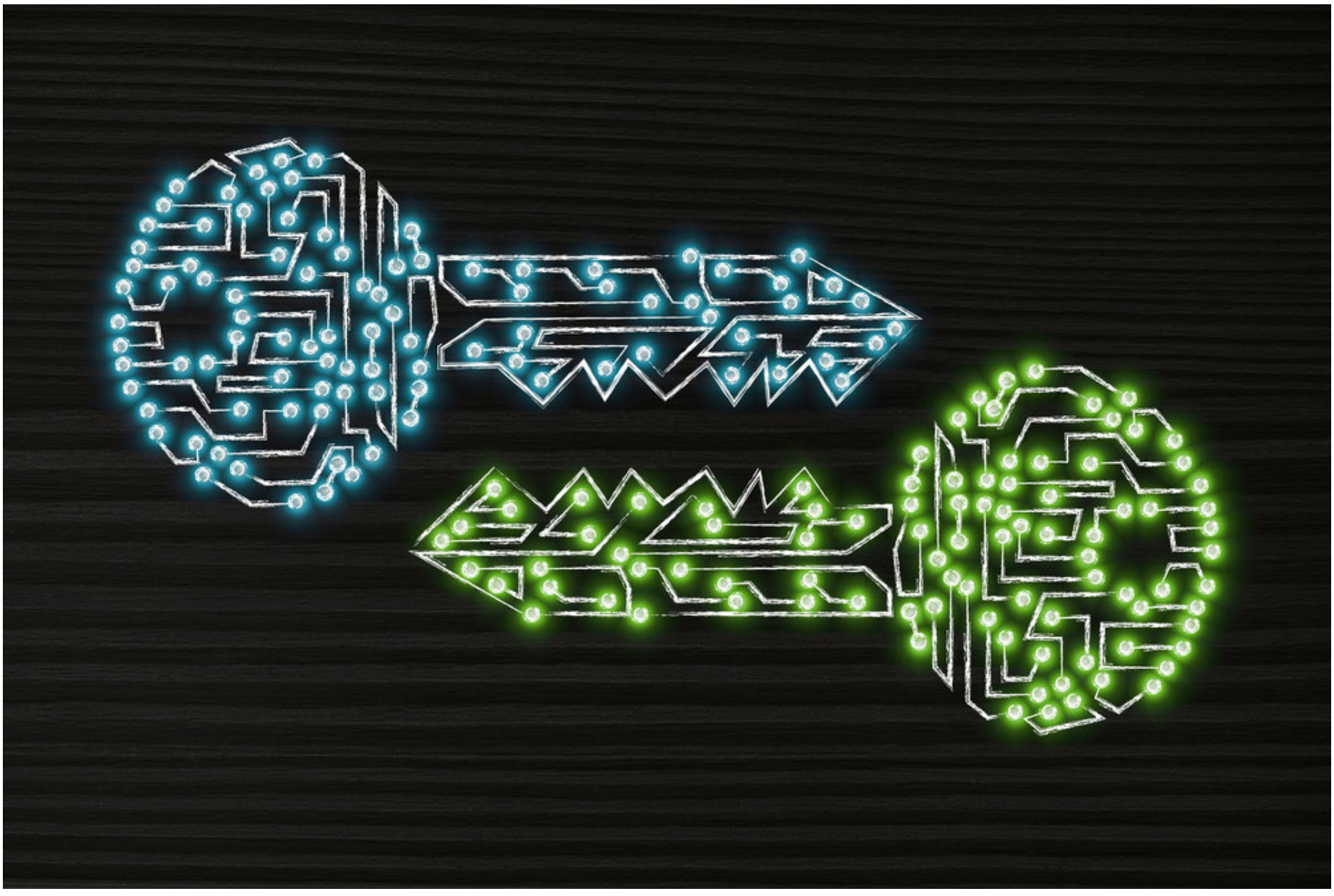
FOCO NO MERCADO DE TRABALHO

CRIPTOGRAFIA

Emilio Tissato Nakamura

APLICAÇÕES DA CRIPTOGRAFIA

A criptografia de chave privada e a criptografia de chave pública têm uma série cada vez maior de aplicações.



Fonte: Shutterstock.

Deseja ouvir este material?

Áudio disponível no material digital.

SEM MEDO DE ERRAR

Você é o responsável pela segurança da informação de uma empresa química e sua apresentação para a diretoria executiva com a estratégia de segurança para as situações relatadas deve, ao mesmo tempo, mostrar que há riscos envolvidos e que você sabe como fazer a empresa avançar.

Comece a apresentação contextualizando o projeto de desenvolvimento do composto químico para o agronegócio e a forma como as equipes estão trabalhando nas três localidades do Brasil (São Paulo, Rio de Janeiro e Salvador), em conjunto com os parceiros chineses e suíços.

A partir do entendimento de como as equipes estão trabalhando, inclua as plataformas, os sistemas e aplicativos utilizados.

Incorpore as ameaças relacionadas com a criptografia para cada uma dessas situações, que envolvem as pessoas, as necessidades e as plataformas, os sistemas e aplicativos. Um direcionamento pode ser:

- **Situação 1:** armazenamento de resultados do projeto no servidor de arquivos na nuvem. Servidor de arquivos ou o provedor de nuvem pode ser atacado e a documentação pode ser vazada ou alterada. Envolve confidencialidade e integridade.
- **Situação 2:** armazenamento de resultados do projeto no serviço de troca de arquivos. Serviço pode sofrer um incidente de segurança e resultar em acesso não autorizado. Envolve confidencialidade e integridade.
- **Situação 3:** armazenamento de documentação em notebooks e *pendrives*. Equipamentos e dispositivos podem ser roubados, perdidos ou acessados indevidamente. Envolve confidencialidade no caso de roubo, perda ou acesso indevido, e integridade no caso de acesso indevido.
- **Situação 4:** dados do projeto trafegam pela Internet quando são trabalhados de forma colaborativa, quando são armazenados no servidor de arquivos e quando são enviados entre as equipes, via e-mail e serviço de troca de

arquivos. Dados podem ser expostos e alterados durante a transmissão. Envolve confidencialidade e integridade.

- **Situação 5:** dados do projeto trocados via e-mail permanecem nestes servidores, que podem ser atacados. Envolve confidencialidade e integridade.
- **Situação 6:** origem dos documentos pode ser alterada, de modo que informações falsas podem ser inseridas na empresa. Envolve integridade e, mais especificamente, autenticidade de origem.

Ver anotações

A estratégia de segurança envolvendo a criptografia pode ser definida desta forma:

- Criptografia de chave privada ou simétrica: situações 1, 2, 3, 4, 5 e 6.
- *Hash* criptográfico: situações 1, 2, 3, 4, 5 e 6.
- Criptografia de chave pública ou assimétrica com assinatura digital: situação 6.

Não se esqueça de incluir um *overview* sobre os tipos de criptografia na apresentação para a diretoria executiva.

AVANÇANDO NA PRÁTICA

UM DOCUMENTO SECRETO PARA 30

Você é o especialista de segurança de um conglomerado de agentes secretos, com uma série de atividades, e sua função é proteger a comunicação entre eles. Esses agentes secretos estão espalhados pelo Brasil, e o diretor do conglomerado precisa enviar um comunicado importante, sensível e secreto para 30 do total de 31 agentes secretos. Qual é a sua estratégia para que os 30 agentes secretos, e somente eles, recebam o comunicado?

RESOLUÇÃO

Você poderia propor o uso de criptografia para proteger o comunicado. Sim, a criptografia faz sentido, mas o de chave privada ou simétrica traz alguns desafios. Como você faria a distribuição desta chave privada para os 30 agentes secretos, mais o diretor? E, se a chave privada deve chegar de forma

secreta para cada um dos 30 agentes secretos, por que já não enviar o comunicado? Eles já estão espalhados pelo Brasil, e um encontro físico e real poderia resolver o problema das chaves, mas neste caso também a criptografia seria desnecessária, já que o próprio comunicado poderia ser entregue pessoalmente.

Outro ponto importante da criptografia de chave privada é que, em caso de comprometimento da chave privada, todos estarão inseguros, com uma nova chave privada tendo de ser definida. Neste caso de muitas entidades (30 agentes secretos), a criptografia de chave privada apresenta limitações.

A melhor solução é o uso da criptografia de chave pública. O diretor e cada um dos 31 agentes secretos poderiam ter um par de chaves. Para o comunicado, o diretor pode utilizar as chaves públicas dos 30 agentes secretos com quem ele precisa se comunicar. Cada um deles, assim, recebe o pacote cifrado e é o único que pode decifrá-lo, já que somente ele possui a chave privada correspondente.