Nome: Eduardo Cunha

Criptografia

Imagine um palco onde as cortinas são feitas de partículas subatômicas. Atrás delas, duas pessoas estão encenando uma peça, mas só as sombras projetadas por uma luz mutável chegam à plateia. Cada movimento dos atores é traduzido em formas distorcidas, indecifráveis sem o conhecimento exato da fonte de luz, da posição dos corpos e do material das cortinas. Essa projeção é o que um espião veria — dados criptografados.

Agora, a chave para entender a peça não é apenas um script, mas uma coreografia secreta entre os dançarinos e a física do espaço em que eles estão. Mude qualquer variável — o tempo da apresentação, a densidade das cortinas, o ângulo da luz — e tudo perde sentido. Na criptografia real, essa coreografia é feita com matemática, mas a ideia é a mesma: tornar a mensagem ilegível a menos que você saiba exatamente como foi encenada.

O que torna essa peça mais fascinante: às vezes, os dançarinos (ou algoritmos) mudam a coreografia a cada apresentação, como na criptografia assimétrica. Outras vezes, usam o mesmo passo para cada número, como na simétrica. Mas sempre dançam para esconder — e só quem tem a senha da música ouve a melodia real.

Chave simétrica

Imagine duas pessoas atravessando um deserto silencioso. Cada uma carrega um instrumento musical — mas os instrumentos são idênticos, afinados exatamente da mesma forma. Não há palavras entre elas, apenas sons. Uma toca uma melodia específica, complexa, repleta de pausas e harmonias. A outra, a quilômetros de distância, ouve o eco e, por ter o mesmo instrumento e o mesmo conhecimento da afinação, consegue reproduzir exatamente a mesma melodia — e assim entender a mensagem.

Esse deserto não tem ruídos. Mas, para qualquer estranho que escute, a melodia é apenas um som bonito e desconexo. Só quem carrega o instrumento certo, afinado exatamente igual, compreende o que está sendo dito. Esse instrumento é a chave simétrica.

Agora, aqui está o detalhe que poucos notam: se um terceiro roubar o instrumento de um deles, tudo desmorona. A segurança depende não da complexidade da melodia, mas do sigilo do instrumento. Por isso, antes mesmo de começarem a tocar, essas duas pessoas precisam se encontrar em segredo e afinar seus instrumentos juntos — o momento mais frágil de toda a jornada.

Essa é a essência da criptografia simétrica: dois lados com a mesma chave, tentando manter a música fora do alcance de ouvidos estranhos, em um deserto onde cada som é valioso, mas só faz sentido para quem compartilha o mesmo segredo.

Chave assimétrica

Imagine uma cidade flutuando no céu. Cada casa tem uma porta especial: qualquer um pode fechá-la, mas apenas o morador pode abri-la. Essas portas são forjadas com uma geometria tão estranha que o ato de fechar (trancar) é fácil e público — mas o mecanismo de abertura é privado, único, e praticamente impossível de ser reproduzido sem o metal exato escondido no bolso do morador.

Agora pense assim: você quer mandar uma carta para alguém nessa cidade. Você não precisa conhecer o segredo da porta — basta usar a estrutura dela para trancar sua carta dentro. Só o dono daquela porta, com sua chave interior, pode abri-la. E o mais curioso: o próprio morador pode trancar mensagens para você usando a sua porta, sem jamais saber como você abre a sua.

Essa é a essência da criptografia assimétrica: **duas chaves**, como dois lados de uma mesma porta mágica — uma pública, que

qualquer um pode usar para trancar, e uma privada, guardada com zelo, usada apenas para abrir.

É um sistema onde confiança não depende de segredo compartilhado, mas de **segredo individual**. Uma arquitetura onde as portas estão abertas para receber, mas blindadas para manter o que entra só visível a quem tem o direito.

E mais: essas casas se comunicam entre si com portas duplas — um envia, o outro assina, o outro verifica, o primeiro confirma. Tudo sem nunca trocar o metal das chaves. Apenas ecos do formato da porta.