**Criptografia Quântica**

Criptografia se refere ao estudo e prática de princípios e técnicas (geralmente protocolos) que tornam as informações seguras. O principal objetivo da criptografia é permitir a comunicação segura entre um emissor (Alice), e um receptor (Bob) sem que um adversário (Eve) possa ler as mensagens.

Na Criptografia Clássica, é possível, por exemplo, utilizar os protocolos de chave pública e chave privada: Alice precisa enviar a Bob sua chave pública. A chave pública criptografa a mensagem de forma que a chave privada possa descriptografá-la. Bob então usa a chave que recebeu de Alice para criptografar a mensagem, e a envia. Eve, que está escutando a conversa, conseguiu ter acesso tanto à chave pública quanto à mensagem. Entretanto, a chave pública não descriptografa a mensagem, apenas a chave privada o faz. Assim, a comunicação parece continuar segura.

Porém, essa segurança não é matematicamente comprovada, e toda a sua segurança teórica depende da alta complexidade de algum problema matemático.

Por exemplo, o protocolo RSA funciona da maneira descrita acima, sendo sua chave pública a combinação de dois números primos muito grandes, e um valor auxiliar (*n, e* | *n* = *pq*, sendo *p* e *q* dois primos muito grandes que devem ser mantidos privados). A chave privada é outro número (*d*), que permite calcular *p* e *q* (na implementação, geralmente a chave privada já vem como o conjunto *p ,q, d* de forma a acelerar os cálculos) e descriptografar a mensagem.

Toda a segurança do RSA depende de Eve não ser capaz de calcular *p* e *q* em função de *n* em tempo hábil (geralmente cada um com 1024 bits). Usando computação clássica, levaria milhares de anos para verificar quais primos foram utilizados. Mas com computação quântica, isso pode ser quebrado em menos de uma hora, utilizando por exemplo o algoritmo de Shor.

Mas a própria computação quântica oferece uma resposta a esse problema. A Criptografia Quântica propõe uma maneira diferente de olhar para a criptografia no geral: Baseando-se principalmente no Princípio de Incerteza de Heisenberg (PIH), um espião não pode ter acesso à chave pública sem, ao mesmo tempo, denunciar sua presença. Constrói-se, assim, um canal quântico de comunicação.

Nessa nova comunicação, Alice envia a Bob a sua chave pública. Porém, agora Eve não pode ter acesso sequer à essa chave, pois tem em mãos uma máquina muito potente que poderia destruir a criptografia. Mas Bob e Alice, sabendo disso, estão utilizando um canal quântico de comunicação. Nesse canal, se Eve interceptar a chave, vai involuntariamente fazer uma alteração nela, o que vai denunciá-la aos interlocutores, que podem então reformular o canal que estão utilizando e trocar as chaves, tornando a informação que Eve conseguiu inútil.

Referências:

* [https://pt.wikipedia.org/wiki/Criptografia\_de\_chave\_p%C3%BAblica](https://pt.wikipedia.org/wiki/Criptografia_de_chave_pública) Acesso em: 10 de março de 2020.
* [https://pt.wikipedia.org/wiki/Criptografia\_qu%C3%A2ntica](https://pt.wikipedia.org/wiki/Criptografia_quântica) Acesso em: 10 de março de 2020.
* <https://issuu.com/arlufla/docs/mono-andersonoliveira> Acesso em: 14 de março de 2020.
* <https://pt.wikipedia.org/wiki/Criptografia> Acesso em: 14 de março de 2020.
* <http://www.scielo.br/scielo.php?pid=S0102-47442005000400004&script=sci_arttext&tlng=pt> Acesso em: 14 de março de 2020.
* <https://canaltech.com.br/seguranca/criptografia-para-iniciantes-o-que-e-como-funciona-e-por-que-precisamos-dela-46753/> Acesso em: 14 de março de 2020.
* <https://researcher.watson.ibm.com/researcher/files/us-bennetc/BB84highest.pdf> Acesso em: 15 de março de 2020.
* <https://monografias.brasilescola.uol.com.br/computacao/aplicacao-computacao-quantica-na-resolucao-problemas-computacionais-impacto-cientifico.htm> Acesso em: 14 de março de 2020.
* [https://www.researchgate.net/profile/Armando\_Faz\_Hernandez/publication/ 285587792\_Implementacao\_Eficiente\_e\_Segura\_de\_Algoritmos\_Criptograficos/links/566064d308ae15e7462bd8e3/Implementacao-Eficiente-e-Segura-de-Algoritmos-Criptograficos.pdf](https://www.researchgate.net/profile/Armando_Faz_Hernandez/publication/285587792_Implementacao_Eficiente_e_Segura_de_Algoritmos_Criptograficos/links/566064d308ae15e7462bd8e3/Implementacao-Eficiente-e-Segura-de-Algoritmos-Criptograficos.pdf) Acesso em: 15 de março de 2020.