SEGURANÇA DA INFORMAÇÃO E DE REDES

Prof. Milton Palmeira Santana

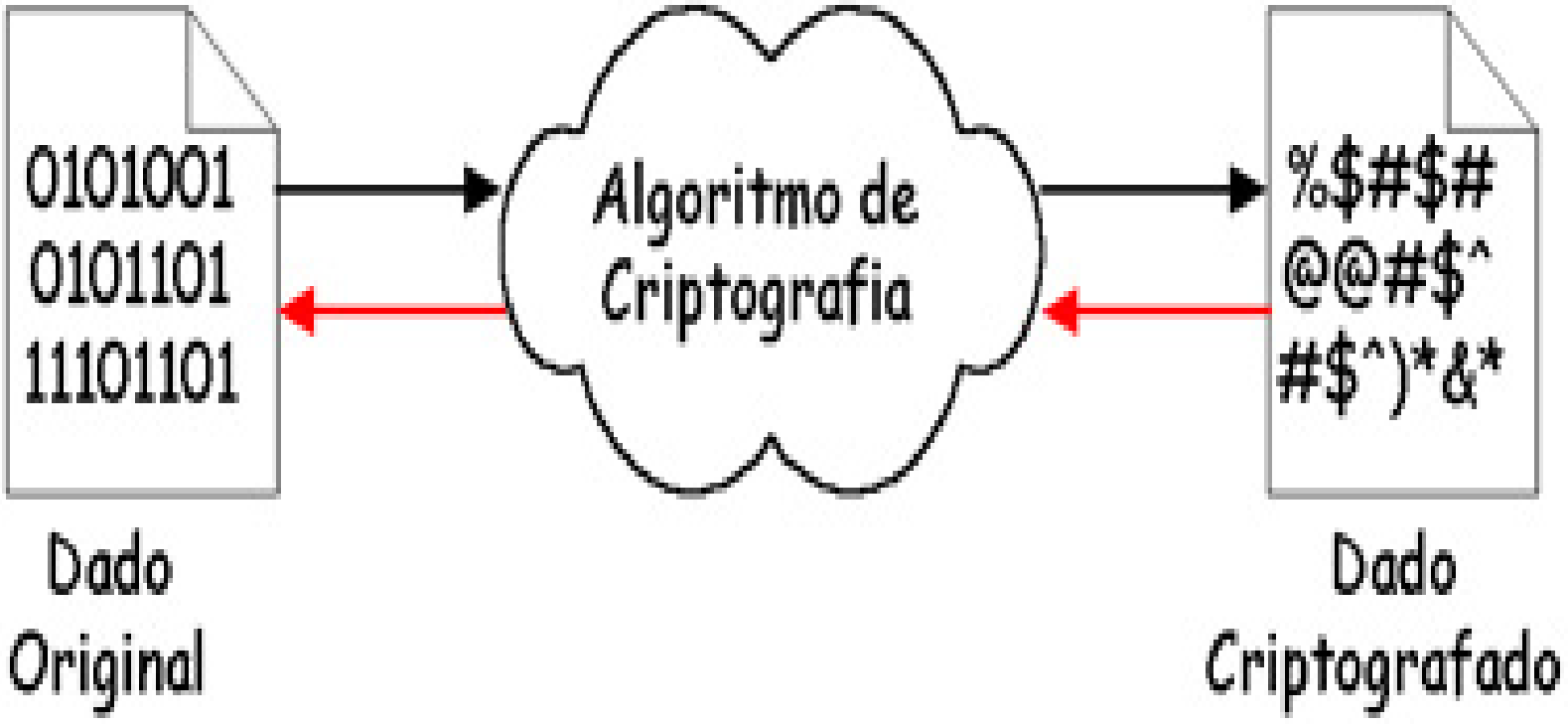
Conceitos

- Criptografia, portanto, é o ato de alterar a mensagem para esconder o significado desta.

- Mas como esconder?
  - Criando cifras.

Conceitos

- Os procedimentos de criptografar e descriptografar são obtidos através de um **algoritmo de criptografia**.



Conceitos

- Imagine que Alice quer enviar uma mensagem para Beto por um canal, que normalmente é inseguro. Nesse canal um atacante pode escutar a mensagem, afetando a privacidade ou a confidencialidade da comunicação entre Alice e Beto.

- Com o uso da criptografia, Alice pode enviar uma mensagem cifrada para Beto. Alice utiliza um algoritmo criptográfico que utiliza uma chave secreta para cifrar a mensagem original. O resultado é um texto incompreensível para o atacante. Beto recebe a mensagem cifrada e utiliza a mesma chave secreta (compartilhada com Alice) para decifrar a mensagem e chegar ao conteúdo original.

Conceitos

- Esse é o funcionamento básico da criptografia simétrica ou de chave privada, em que a chave secreta é a mesma para a cifragem e decifragem e que, portanto, deve ser compartilhada.

- Os processos de cifragem e decifragem são realizados via uso de algoritmos com funções matemáticas que transformam os textos claros, que podem ser lidos, em textos cifrados, que são ininteligíveis.

- Um exemplo de criptografia, bastante simples, é o ROT-13, que é uma cifra de substituição que troca cada letra da mensagem por uma que está 13 posições à frente no alfabeto. Uma mensagem de Alice para Beto com o conteúdo “Oi” viraria, com o uso do ROT-13, “Bv”, já que “O” é substituída por “B”, que está 13 posições à frente, e “i” é substituída por “v”.

Conceitos

- Os objetivos básicos da criptografia são:
  - **Sigilo**: proteção dos dados contra divulgação não autorizada.
  - **Autenticação**: garantia que a entidade se comunicando é aquela que ela afirma ser.
  - **Integridade**: garantia que os dados recebidos estão exatamente como foram enviados por uma entidade autorizada.
  - **Não repúdio**: garantia que não se pode negar a autoria de uma mensagem.
  - **Anonimato**: garantia de não rastreabilidade de origem de uma mensagem.

Segurança dos sistemas criptográficos

- A segurança da criptografia não pode ser medida somente pelo tamanho da chave utilizada, sendo necessário conhecer o algoritmo e a matemática envolvida no processo de codificação de dados. Desse modo, um algoritmo que utiliza chaves de 256 bits não significa que é mais seguro do que outros algoritmos, como o DES de 128 bits, caso existam falhas no algoritmo ou em sua implementação.

- Há a possibilidade de atacar uma informação protegida com criptografia pelo algoritmo ou pela descoberta da chave secreta.

- O algoritmo RC4 já foi pivô de problemas no WEP (Wired Equivant Privacy), protocolo de segurança utilizado em redes Wi-Fi em 2001. Já em 2013, o TLS/SSL teve uma grave falha de segurança divulgada relacionada ao mesmo algoritmo RC4.

Segurança dos sistemas criptográficos

- O DES (Data Encryption Standard) teve sua efetividade invalidada em 1997, quando uma mensagem cifrada com o algoritmo foi quebrado pela primeira vez. Os custos dos equipamentos que realizavam o ataque de força bruta foram diminuindo, ao mesmo tempo em que o tempo para a quebra também foi sendo drasticamente reduzida. Em 1998, um equipamento com custo de US$ 250 mil quebrou uma chave de 56 bits em aproximadamente dois dias.

- Curiosidade: o DES foi criado por volta de 1975.

Segurança dos sistemas criptográficos

- A segurança de sistemas criptográficos depende de uma série de fatores, tais como:
  - **Geração de chaves**: sem uma geração aleatória de chaves, o algoritmo utilizado pode revelar padrões que diminuem o espaço de escolha das chaves, o que facilita a sua descoberta.
  - **Mecanismo de troca de chaves**: as chaves precisam ser distribuídas e trocadas para o estabelecimento das comunicações seguras e, para tanto, protocolos como o Diffie-Hellman são utilizados. Esse protocolo será discutido nas próximas aulas.

Segurança dos sistemas criptográficos

- A segurança de sistemas criptográficos depende de uma série de fatores, tais como:
  - **Taxa de troca das chaves**: quanto maior a frequência de troca automática das chaves, maior será a segurança, pois isso diminui a janela de oportunidade de ataques, pois, caso uma chave seja quebrada, em pouco tempo ela já não é mais útil para a comunicação.
  - **Tamanho da chave**: são diferentes para a criptografia de chave privada ou simétrica e para a criptografia de chaves públicas ou assimétricas.

Segurança dos sistemas criptográficos

- Pense em um algoritmo criptográfico e a chave que protege determinada informação. É mais fácil quebrar o código (algoritmo) ou encontrar a chave?

- Um dos métodos para se quebrar a chave criptográfica é o ataque de força bruta, em que diferentes combinações são testadas.

- Vamos descriptografar o código abaixo:

- **%&$**

- AAA
- AAB

História

- A história da criptografia é composta por grandes eventos.
- O primeiro uso documentado da criptografia foi em torno de 1900 a.C., no Egito, quando um escriba usou hieróglifos fora do padrão numa inscrição.
- Já entre 600 a.C. e 500 a.C., os hebreus utilizavam a cifra de substituição simples, que era fácil de ser revertida com o uso de cifragem dupla para obter o texto original.
- A Cifra de César é um dos exemplos mais clássicos de criptografia, em que as substituições eram feitas com as letras do alfabeto avançando três casas.

História – Criptografia clássica

- Historicamente, os métodos clássicos de criptografia são divididos em duas técnicas:
  - Cifras de substituição
  - Cifras de transposição
- Na transposição as letras das mensagens são simplesmente rearranjadas, gerando, efetivamente um anagrama.
- Para mensagens muito curtas, esse método é relativamente inseguro. Por exemplo, uma palavra de três letras só pode ser rearranjada de seis maneiras diferentes. Exemplo: ema, eam, aem, mea, mae, ame.

História – Criptografia clássica

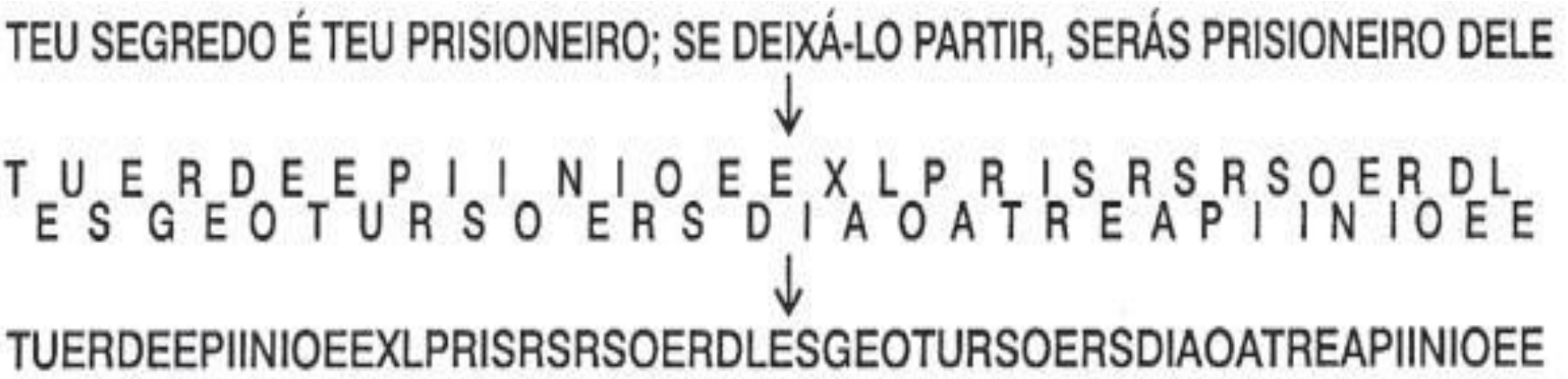
- Entretanto, se o número de letras aumenta, o número de arranjos aumenta muito.

- **Como exemplo vamos considerar esta frase**. Ela contém apenas 35 letras, mas existem 50.000.000.000.000.000.000.000.000.000.000 de arranjos distintos.

- Curiosidade: se uma pessoa pudesse verificar uma disposição por segundo, e se todas as pessoas no mundo trabalhassem dia e noite, ainda assim levaria mais de mil vezes o tempo do universo para checar todos os arranjos possíveis.
- **Fonte: O livro dos códigos Simon Singh (2007, 6ª edição)**

História – Criptografia clássica

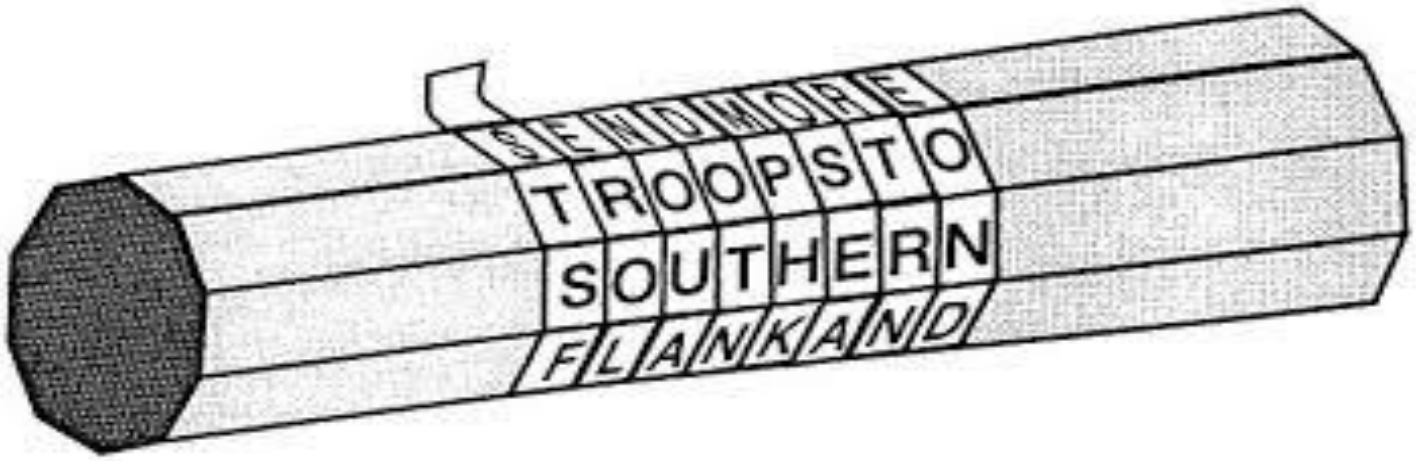
- Exemplo transposição da “cerca de ferrovia”: envolve escrever uma mensagem de modo que as letras alternadas fiquem separadas nas linhas de cima e de baixo. A sequência de letras na linha superior é então seguida pela inferior, criando a mensagem cifrada final. **Exemplo**:



História – Criptografia clássica

- O receptor pode recuperar a mensagem simplesmente revertendo o processo. Existem várias formas de transposição sistemática, incluindo a cifra de três linhas.

- Outra forma de transposição envolve o primeiro aparelho criptográfico miliar, o **citale espartano**, que data do século cinco antes de cristo. Consiste em um bastão de madeira em volta do qual é enrolada uma tira de couro ou pergaminho.



História – Criptografia clássica

- A alternativa para a transposição é a substituição.
- As cifras de substituição preservam a ordem dos símbolos no texto claro, mas disfarçam esses símbolos.
- Cada letra ou grupo de letras é substituído por outra letra ou grupo de letras, de modo a criar um “disfarce”.
- **CURIOSIDADE**: uma das primeiras descrições de código por substituição aparece no **Kama-sutra**. O texto data do século IV a.C.

História – Criptografia clássica

- O primeiro documento que usou uma cifra de substituição para propósitos militares aparece nas guerras da Gália de Júlio César.

- A Cifra de César, também conhecida como cifra de troca, código de César ou troca de César, é uma das mais simples e conhecidas técnicas de criptografia. É um tipo de cifra de substituição na qual cada letra do texto é substituída por outra, que se apresenta no alfabeto abaixo dela um número fixo de vezes.

- O nome do método é em homenagem a Júlio César, que o usou para se comunicar com os seus generais.

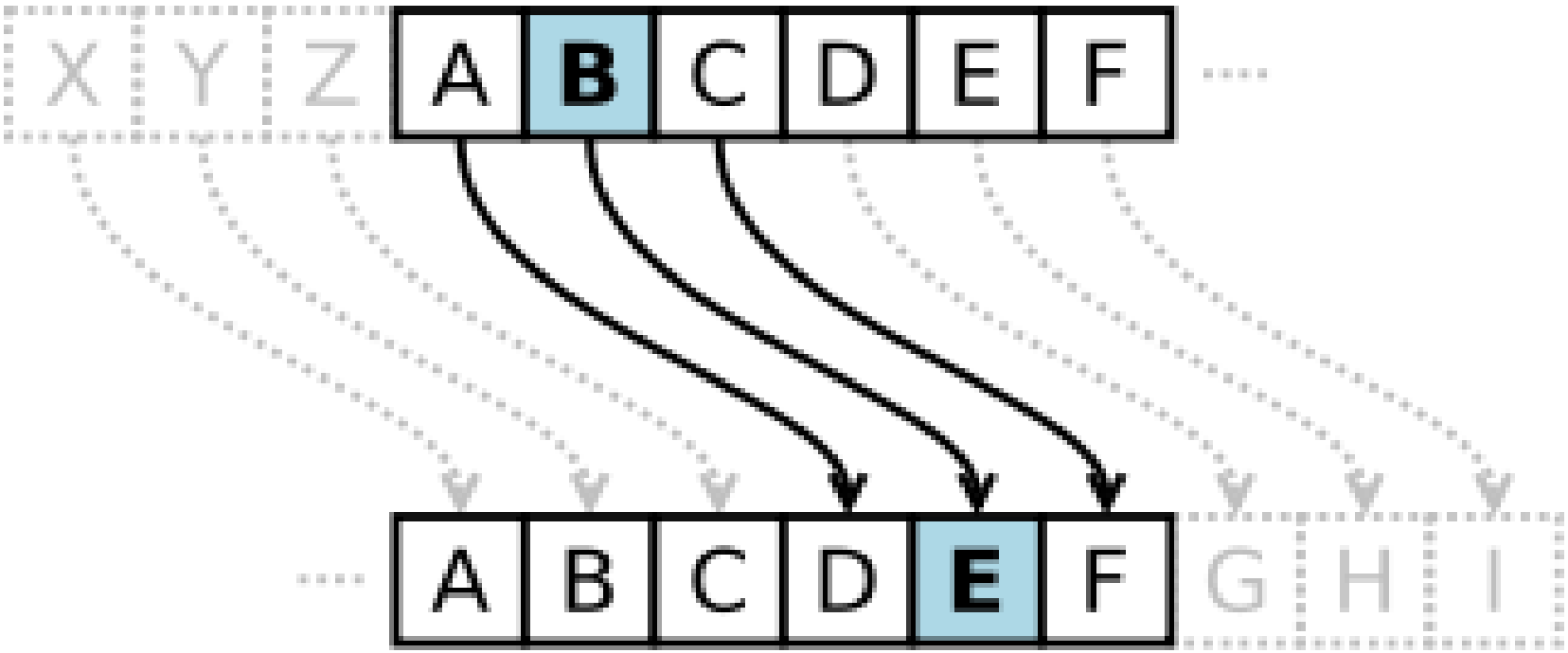
História – Criptografia clássica

- Considerando as 26 letras do alfabeto

  (a,b,c,d,e,f,g,h,I,j,k,l,m,n,o,p,q,r,s,t,u,v,w,x,y,z),

- Neste método, **a** se torna **D**, **b** se torna **E**, **c** se torna **F**, … …, **z** se torna **C**.

História – Criptografia clássica



História – Criptografia clássica

- EXEMPLO:

C O M P U T A C A O

F R P S X W D F D R

EXERCÍCIO – 10 min

Crie uma frase com pelo menos 3 palavras.

Utilize Criptografia de César. (Quantas casas quiser).

História – Criptoanálise

- A criptoanálise é a arte de tentar descobrir o texto cifrado e/ou a lógica utilizada em sua encriptação (chave). As pessoas que participam desse esforço são denominadas criptoanalistas. Da fusão da criptografia com a criptoanálise, forma-se a criptologia.

- A criptoanálise representa o esforço de decodificar ou decifrar mensagens sem que se tenha o conhecimento prévio da chave secreta que as gerou.

EXERCÍCIO – 15 min

DECODIFIQUE A MENSAGEM.

PXLWDV YHCHV WHQWHL IXJLU GH PLP, PDV DRQGH HX LD HX WDYD

RESOLUÇÃO


"Muitas vezes
tentei fugir
de mim, mas
aonde eu ia,
eu tava"
Tiririca

História

- Com a Cifra de Vigenère a evolução consistiu no uso de diferentes valores de deslocamento para as substituições.
- A criptoanálise, que buscava padrões que identificavam mensagens ocultas, cresceu na Idade Média.

- Já a máquina criada pelo alemão Kasiski, o Enigma, foi utilizada para a segurança das comunicações na Segunda Guerra Mundial. O Enigma era uma máquina física, assim como o Colossus, que conseguiu decifrar mensagens do Enigma após uma engenharia reversa a partir de uma máquina furtada.

- Um avanço importante foi a criação de criptografia de chave pública, em 1976, por Diffie e Hellman, que levou ao desenvolvimento do algoritmo RSA.

História

- Antes, da proteção de comunicação em guerras; hoje a criptografia faz parte do cotidiano de todos, muitas vezes de uma forma transparente, como é o caso do acesso web, de transações bancárias e de acesso às redes.

Uso atual da criptografia

- A Apple, por exemplo, utiliza práticas de segurança-padrão do setor e emprega rígidas políticas para proteção dos dados.

- A segurança dos dados e a privacidade das informações pessoais do iCloud (serviço de nuvem da Apple), que é acessado a partir de diferentes dispositivos, trata de diferentes tipos de dados, tanto em trânsito quanto armazenados no servidor. Dados do usuário, por exemplo, são protegidos com a criptografia AES de, no mínimo, 128 bits. Já a criptografia AES de 256 bits é utilizada para armazenar e transmitir senhas e informações de cartões de crédito. Além disso, a Apple também usa criptografia assimétrica de curva elíptica e empacotamento de chave.

Uso atual da criptografia

- Já o serviço de mensagens WhatsApp começou em abril de 2016 a utilizar criptografia em todas as suas comunicações, incluindo mensagens de voz e outros arquivos, entre seus usuários. Com o que chamam de "criptografia de ponta a ponta", as mensagens são embaralhadas ao deixar o telefone da pessoa que as envia e só conseguem ser decodificadas no telefone de quem as recebe. Segundo um comunicado da empresa, “Quando você manda uma mensagem, a única pessoa que pode lê-la é a pessoa ou grupo para quem você a enviou. Ninguém pode olhar dentro da mensagem. Nem cibercriminosos. Nem hackers. Nem regimes opressores. Nem mesmo nós".

EXERCÍCIOS

1, 2 e 3 do Livro.

REFERÊNCIAS

MACHADO, Felipe Nery Rodrigues. **Segurança da Informação: princípios e controle de ameaças**. [S. l.]: ÉRICA, 2014.

FONTES, Edison. **Segurança da Informação**: O usuário faz a diferença. [S. l.]: SARAIVA, 2007.

SMULDERS, André; BAARS, Hans; HINTZBERGEN, Jule; HINTZBERGEN, Kees. **Fundamentos de Segurança da Informação**: com base na ISO 27001 e na ISO 27002. [S. l.]: BRASPORT, 2018.

BASTA, Alfred; BASTA, Nadine; BROWN, Mary. **Segurança de computadores e teste de invasão**. [S. l.]: Cengage Learning, 2014.

REFERÊNCIAS

GOODRICH, Michael T.; TAMASSIA, Roberto. **Introdução à Segurança de Computadores**. [S. l.]: Bookman Editora, 2013.

STALLINGS, WILLIAM. **Criptografia e Segurança de Redes**: Princípios e práticas. 6. ed. [S. l.]: Pearson Universidades, 2014.

SINGH, Simon. **O livro dos códigos**: A ciência do sigilo – do antigo Egito à criptografia quântica. [S. l.]: Record, 2001.


Anhanguera