Aula 19: Criptografia

Prof. Sérgio Montazzolli Silva
smsilva@uel.br

Nesta aula

- Criptografia
- Chaves de Acesso
- HTTPS
- SSL

Imagine

- Imagine que, no ano de 1732
  Maria quer enviar uma mensagem a João, e
  esta mensagem não pode ser lida por ninguém,
  a não ser o próprio João
- Porém, a única forma de enviar a mensagem é através de Mateus, que está indo para a cidade de João
- É muito importante que Mateus não leia esta mensagem e, principalmente, não a adultere
- Como Maria poderia fazer isso?

Exemplo

- Quando se encontraram, muito esperta, Maria combinou com João que todas as palavras da mensagem estariam escritas de trás para frente
- Por exemplo:
  - Mensagem: "somav son rartnocne an adineva sa h01"
- Qual é a mensagem que deve chegar a João?
  - Resposta: "vamos nos encontrar na avenida as 10h"
- Você considera essa codificação como forte ou vulnerável?

Exemplo

- José, muito esparto também, conseguiu compreender a mensagem, e adulterou o seu conteúdo, causando um desencontro entre Maria e João
- Mas Maria não se deu por vencida, combinou mais uma regra com João: “agora iremos somar duas letras a cada letra”...
  - Por exemplo: A --> C, B -->D, C --> E e assim por diante
  - O mesmo para os dígitos
  - As letras Y e Z devem ser codificadas como Y-->A, Z-->B
  - E os dígitos 8 e 9, como 8-->0, 9-->1

Exemplo

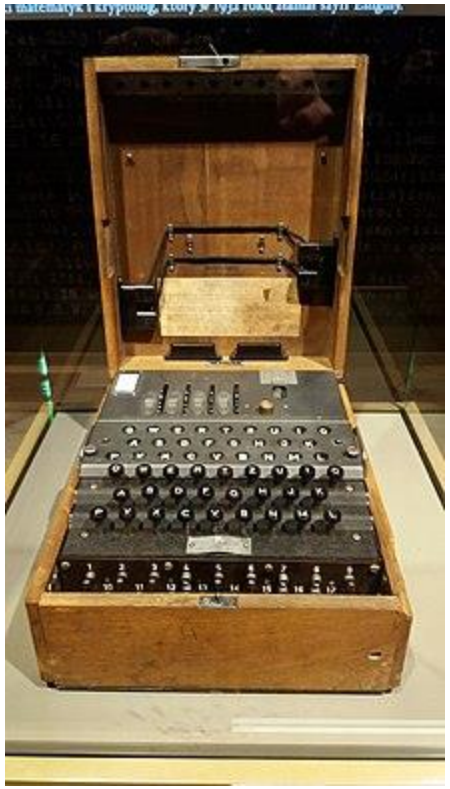
- Agora a nova mensagem ficou?
  - "uqocx uqp tctvpqepg cp cfkpgxc uc j23"
- E agora, está é uma codificação forte ou fraca?
  - Talvez para 1732 fosse um ótima forma de criptografia
  - Porém, atualmente computadores podem testar bilhões de codificações diferentes por segundo
  - Um bom analista poderia descobrir esta codificação em questão de segundos

O que é?

- "*Criptografia é a ciência de manter segredos em segredo*" - Hans Delfs & Helmut Knobi
- O objetivo da criptografia é *manter a confidencialidade da informação enviada*, seja ela texto, números, ou qualquer outro tipo de informação
- Isto é feito a partir da codificação, ou encriptação, da informação original, gerando uma nova mensagem
- Uma mensagem encriptada, mesmo que interceptada, não poderá ser facilmente decifrada

Um pouco de história

- Mensagens criptografadas sempre foram (e ainda são) amplamente utilizadas em guerras
- Durante a 2ª Guerra Mundial, a alemanha nazista utilizava máquinas chamadas de Enigma para encriptar suas mensagens
- Desta forma, os aliados, mesmo conseguindo interceptar as mensagens, não as compreendiam



Um pouco de história

- Nesta época foi quando surgiu o nome de **Alan Turing**, um promissor matemático e criptoanalista inglês
- Ele projetou máquinas e técnicas capazes de decifrar mensagens alemãs criptografadas
- Estima-se que, graças a seu trabalho, a 2ª Guerra Mundial foi encurtada em até 2 anos
- Antes disso, em 1936, Turing havia apresentado a base teórica para o funcionamento de um computador
- Por este último trabalho ele é considerado o **Pai da Computação**

Chaves de Acesso

- A criptografia está presente em vários níveis diferentes, seja em uma transmissão de dados sem fio, seja por fio, ou até mesmo em arquivos pessoais protegidos
- PDFs e outros formatos de arquivo podem vir criptografados e, quando abertos, pedirem uma *chave de acesso*
- **As chaves de acesso são sequências de caracteres utilizadas para criptografar e também decifrar dados**
  - Podem ser entendidas com uma senha

Chaves de Acesso

- Conexões seguras como HTTPS e a encriptação ponta-a-ponta do WhatApp, utilizam chaves de acesso
- Podem haver situações onde existam mais de uma chave de acesso, gerando camadas de criptografia
- Podemos sumarizar o conceito de camadas de criptografia como criptografia aplicada sobre criptografia
  - Simplesmente imagine que a codificação mostrada no inicio da aula (criada por Maria) fosse utilizada 2, 3, 4 ou mais vezes sobre a mesma mensagem
  - Exemplo real: WiFi + HTTPS

HTTP vs. HTTPS

- HTTP: ***Hyper Text*** *Transfer Protocol* ou Protocolo de Transferência de Hyper Texto
  - Protocolo usado para transferência de conteúdo Web, como páginas HTML (***Hyper Text*** *Markup Language*)

- HTTPS: ***Hyper Text*** *Transfer Protocol* *Secure* ou Protocolo Seguro de Transferência de Hyper Texto
  - Exatamente igual a HTTP, porém com uma camada de segurança do tipo SSL

SSL

- SSL é um tipo de protocolo de segurança baseado em:
  - **Chaves de acesso**: permitem que duas máquinas criptografem e decriptografem mensagens entre elas
  - **Certificados**: documento eletrônico de identificação que atesta a validade de uma das partes (normalmente a parte que irá receber informações sensíveis)

SSL – Sequência de Eventos

- Quando uma máquina A quer se conectar a outra máquina B, então B envia a A um certificado digital
- Cabe a máquina A aceitar aquele certificado ou não
- Neste momento entra em cena uma terceira máquina, C, pertencente a alguma entidade certificadora confiável
- A entidade (máquina C) valida ou informa a A que B é realmente possuidora daquele certificado (ou não)
- O certificado sendo válido, a conexão prossegue, utilizando uma chave de acesso gerada pela máquina A, e um cadeado surge no navegador de internet da máquina A