Introdução a Técnicas de Criptografia

PET-CC UFRN

João Victor Malheiros Farias de Aquino
Universidade Federal do Rio Grande do Norte (UFRN)
Pró-Reitoria de Graduação (PROGRAD)

12 de agosto de 2020

Roteiro do seminário

- Introdução
- História da criptografia
  - Cifra de césar
  - Enigma
  - Contemporaniedade
- Criptografia de chave simétrica
  - One-time pad
- Criptografia de chave assimétrica
  - Função Trapdoor
  - Criptografia RSA
- Hashing
  - MD5
- Testes de penetração
  - Kali Linux
  - HashCat
- Conclusão

Introdução

Definição

- A palavra "criptografia" vem do grego *kryptós* (Segredo) + *gráphien* (Escrita);
- É caracterizado como o estudo de técnicas para a realização de troca de informações de uma maneira segura;
- Consiste basicamente em uma série de comandos (algoritmo) para encriptar uma mensagem de modo que apenas o receptor consiga decifrá-la.

História da criptografia

Antiguidade

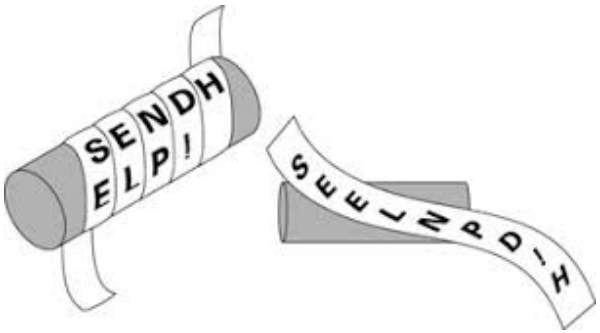
- Por mais que pareça um assunto atual, a criptografia já vem sendo utilizada desde a antiguidade para troca de mensagens (geralmente ligadas a guerra);
- Os primeiros registros da utilização da criptografia datam de 1900 *a.c.* quando foram encontrados hieróglifos nunca antes visto na tumba do nobre egípcio (Knumhotep II). Técnica conhecida como "Symbol Replacement".

Figura 1: Hieróglifo

História da criptografia

Antiguidade

- Em 486 a.c. os espartanos desenvolveram uma técnica para comunicar-se em segurança durante campanhas militares;
- Consiste em uma sequência de caracteres dispostos verticalmente em uma tira de couro que só podem ser lidos ao serem enrolados em uma vara específica.



(a) Cítala desenrolada

(b) Cítala real

História da criptografia

Cifra de César

- Uma das formas mais simples de criptografia, já era utilizada durante o império romano para proteger mensagens militares;
- Essa técnica ficou conhecida como *cifra de césar*;
- Consiste basicamente em substituir a letra pela que está 3 casas na frente.

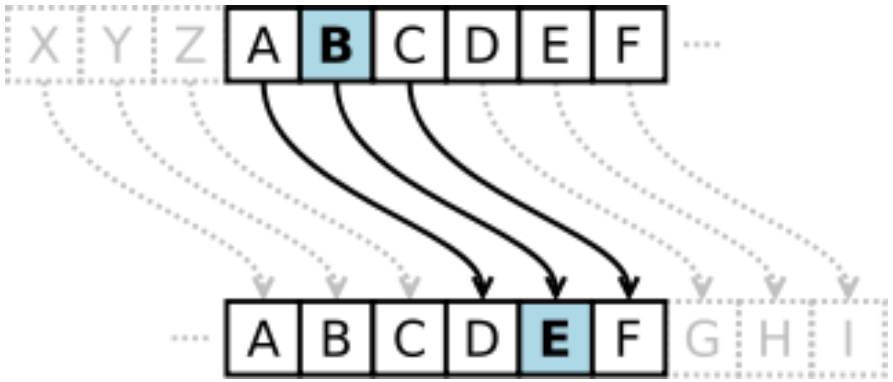
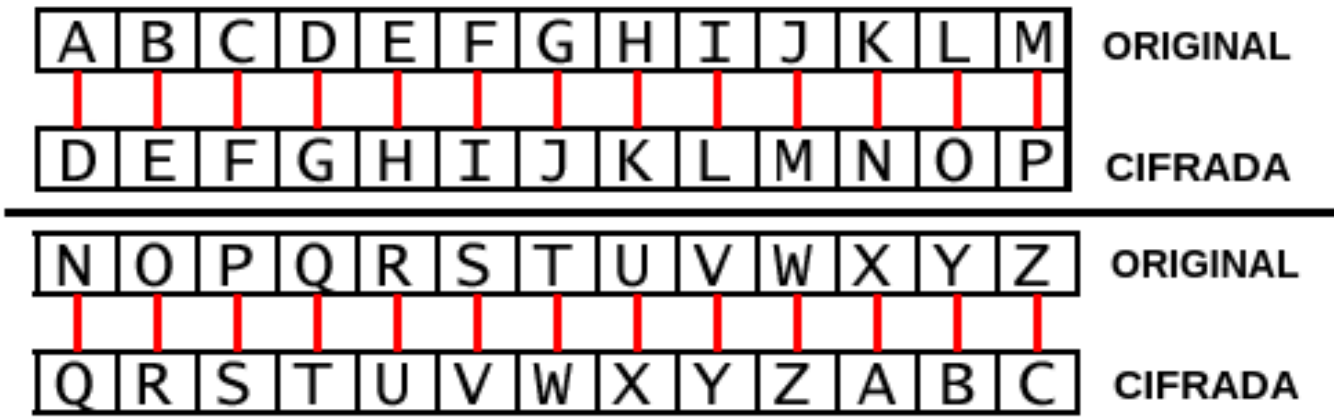


Figura 3: Cifra de César

Cifra de César

Exemplo

Vamos codificar a frase "Olá mundo



O L A M U N D O
R O D P X Q G R

História da criptografia

Máquina Enigma

- Provavelmente a máquina criptográfica mais famosa da história;
- Ela foi usada pelos nazistas durante a segunda guerra mundial para a transmissão de mensagens militares;
- Ela tem um total de 158.962.555.217.826.360.000 combinações possíveis.

Figura 4: Máquina enigma

História da criptografia

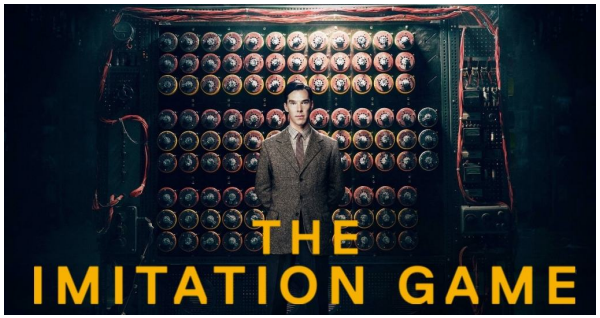
Funcionamento da Enigma

- A máquina tem um rotor eletromecânico que embaralha as letras do alfabeto a cada clique;
- Vídeo;
- Os nazistas recebiam a configuração do dia e usavam para decodar a mensagem;
- Vídeo.

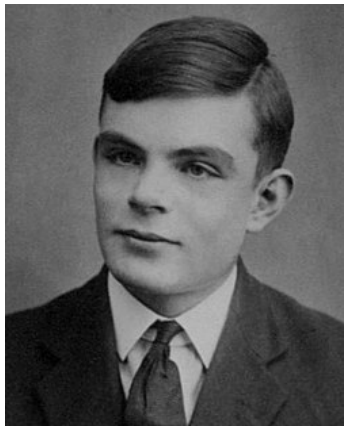
História da criptografia

Quebrando a Enigma

- O cientista da computação britânico *Alan Turing* foi o responsável por conseguir aplicar engenharia reversa de forma a conseguir ter acesso as mensagens secretas dos nazistas;
- A história de *Turing* e da máquina *Enigma* são muito bem retratadas no filme *O jogo da imitação*;
- wetterbericht . . . heil hitler.



(a) O jogo da imitação (2014)



(b) Alan Turing

História da criptografia

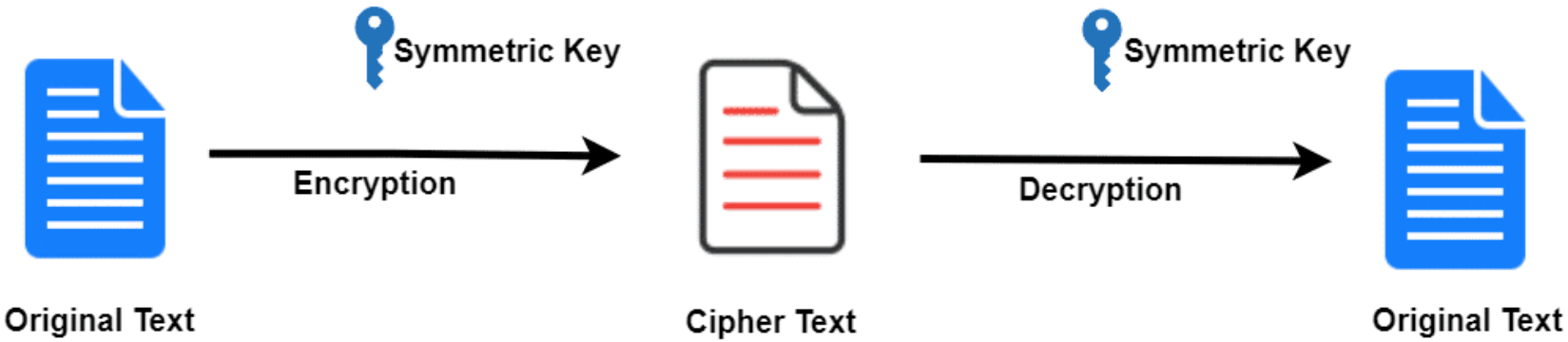
Contemporaneidade

- Atualmente, a criptografia é de fundamental importância para o mundo moderno;
- Ela torna websites seguros e protege nossas informações de terceiros, seja ela uma transferência bancária ou até o envio de um e-mail;
- Sem ela, seria muito mais fácil hackers lerem nossas conversas ou terem acesso a nossa conta bancária.

Criptografia de chave simétrica

Definição

- É um tipo de encripção onde é usado apenas uma chave tanto para encriptar quanto para decriptar;
- Isso não significa nescessariamente que as chaves são iguais, uma pode ser uma transformação simples da outra;
- Quando estudamos *cifra de césar* vimos um exemplo de criptografia de chave simétrica.



Criptografia de chave simétrica

Explicação intuitiva

- Podemos pensar em um algoritmo de chave simétrica da seguinte forma:
  1. Você compra um cadeado na estação de trem com apenas uma chave;
  2. Quando quiser mandar uma mensagem, vá a estação de trem, deixe a mensagem dentro de um armário e tranque ele;
  3. Combine com seu amigo uma data e horário para entregar a chave a ele;
  4. Vá no horário marcado e dê a chave a ele;
  5. Seu amigo vai na estação com a chave, destranca o armário e lê a mensagem;
  6. Para mandar outra mensagem é necessário o mesmo procedimento;
- Conseguem perceber algum problema com esse procedimento?

Criptografia de chave simétrica

Problemas

- O problema é que precisamos enviar a chave por um canal secreto;
- Obviamente se alguém estiver olhando o canal, vai ter a sua chave e poderá ler tudo que você mandar;
- Além disso, para manter um segredo entre 100 pessoas, cada par de pessoas precisaria de sua própria chave, seriam necessárias $\frac{100 \times 99}{2} = 4950$ chaves, dificultando bastante a gestão.

Criptografia de chave simétrica

Vantagens e exemplos

- Vantagens:
  - São muito mais simples de implementar;
  - São mais rápidas;
  - Logo sendo mais utilizidas em encripção em massa, onde segurança não é tão preocupante.
- Exemplos:
  - AES;
  - Twofish;
  - Serpent;
  - Blowfish.

Criptografia de chave simétrica

One-time pad

- Método utilizado pela KGB durante a segunda guerra mundial;
- Consiste em uma única chave em binário;
- Para encriptar utiliza-se um operador binário XOR $\oplus$ entre a mensagem e chave, e para decriptar faz-se o mesmo processo.
- Esse processo funciona, pois aplicando um operador $\oplus$ duas vezes consiste em uma operação nula.

Criptografia de chave simétrica

One-time pad

1. Vamos encriptar a mensagem 01101 com a chave 10110;
2. $10110 \oplus 01101 = 11011$;
3. Enviamos a mensagem encriptada 11011;
4. Ao receber, usamos a mesma chave $10110 \oplus 11011 = 01101$;
5. Chegamos na mensagem original 01101.

Criptografia de chave assimétrica

Definição

- Também conhecida como criptografia de chave pública;
- Consiste em duas chaves, uma pública e uma privada, a pública é sabida por todos, enquanto a privada é exclusiva do receptor;
- A criptografia de chave assimétrica foi criada para tirar a necessidade de envio de chaves secretas como na simétrica.

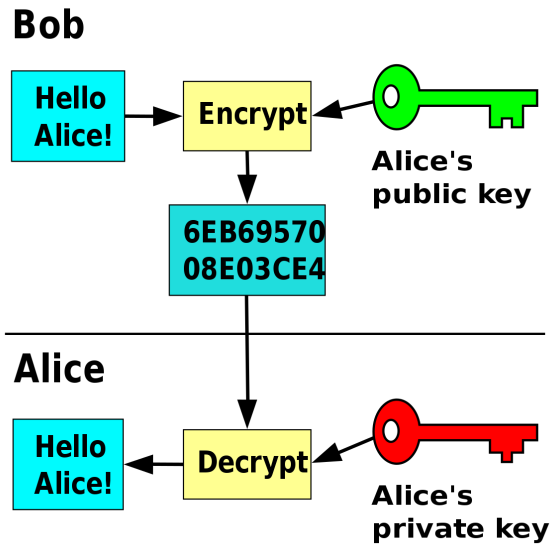


Figura 6: Chave assimétrica

Criptografia de chave assimétrica

Exemplo didático

- Podemos pensar na criptografia de chave assimétrica da seguinte forma:
  1. Alice quer mandar um diamante para Bob por um canal muito inseguro;
  2. Bob envia um cadeado destrancado, que só ele tem a chave, para Alice;
  3. Alice coloca o diamante na caixa, tranca com o cadeado de Bob e envia;
  4. Não importa se alguém mexer na caixa, pois só Bob tem a chave;
  5. Bob recebe a caixa e abre;

Criptografia de chave assimétrica

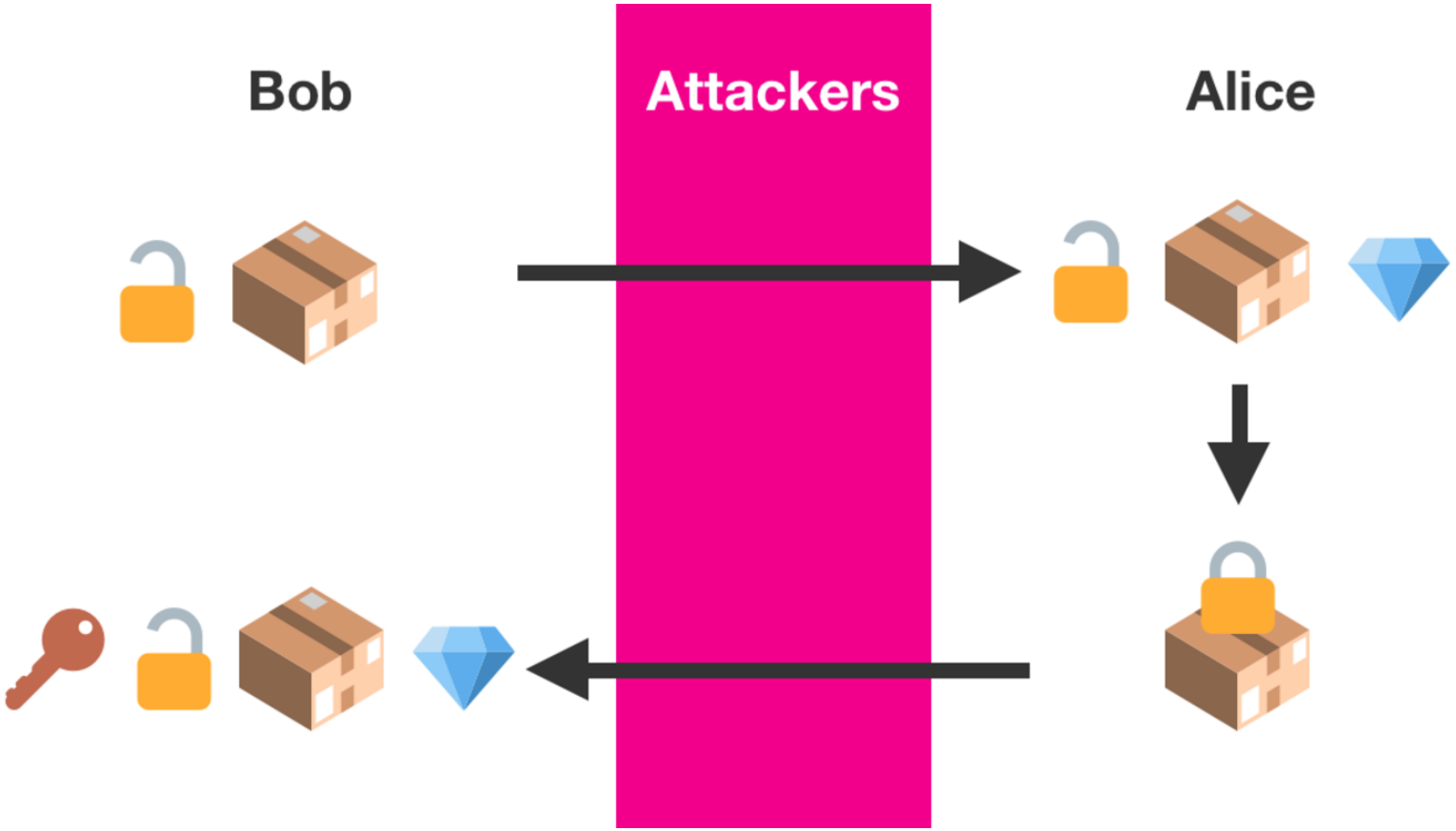


Figura 7: Assimétrica

Criptografia de chave assimétrica

Vantagens, desvantagens e exemplos

- Vantagens:
  1. É mais seguro;
  2. Para manter um segredo entre 100 pessoas, precisaríamos de apenas 200 chaves.
- Desvantagens:
  1. É mais complexo;
  2. É mais demorado.
- Exemplos
  1. Diffie-Helman;
  2. RSA;
  3. Criptografia de curvas elípticas.

Criptografia de chave assimétrica

Função Trapdoor

- *Trapdoor* é um tipo que função que é muito fácil de calcular em uma direção, porém na direção oposta é extremamente complexa;
- Um exemplo de função *Trapdoor* é a multiplicação de dois primos, é muito rápido calcular $17 \times 19 = 323$, mas achar os fatores de 323 é mais complicado.
- Isso se dá pelo fato de existirem algoritmos de tempo polinomial para multiplicação, mas apenas subexponenciais para fatorização

Multiplicação

Curiosidade

- Apesar da fatorização ser um problema trivial, é um problema em aberto na ciência da computação;
- Até agora, não foi encontrado um *lower bound* para o algoritmo mais rápido para multiplicação de inteiros mas é conjecturado que seja[1] $\Omega(n * log(n))$;
- Segue alguns algoritmos descobertos e suas complexidades:
  - Algoritmo *Naive*: $O(n^2)$
  - Algoritmo de *Karatsuba*: $O(n^{log_2 3}) \approx O(n^{1.58})$
  - Toom-3: $O(n^{log_3 5}) \approx O(n^{1.46})$
  - Algoritmo de *Schönhage–Strassen*: $O(n * log(n) * log(log(n)))$

[1] n não representa o número, e sim a quantidade de dígitos dele.

Criptografia de chave assimétrica

Criptografia RSA

- Chaves privadas: p, q primos;
- Chaves públicas: N, e (onde $N = pq$ e $mdc(\varphi(N), e) = 1$);

- Para encriptar a mensagem M:
  1. $enc = M^e \pmod{N}$;
  2. Enviar enc.
- Para decriptar enc:
  1. Achar d tal que $d = e^{-1} \pmod{\varphi(N)}$;
  2. $M = enc^d \pmod{N}$

- Esse método funciona pois $(M^e)^d \equiv M \pmod{N}$

Criptografia de chave assimétrica

Criptografia RSA

- Vamos enviar a mensagem 42;
- Sejam $p = 61$ e $q = 53$;
- Sejam $N = 3233$ e $e = 17$;
  1. $enc = 42^{17} \pmod{3233}$;
  2. $enc = 2557$;
  3. Enviamos 2557;
  4. $\varphi(N) = (61 - 1)(53 - 1) = 3120$
  5. $2753 = 17^{-1}; \pmod{3120}$;
  6. $2557^{2753} \pmod{3233} = 42.$

Hashing

Funcionamento

- Hashing é uma técnica de criptografia que faz uso de uma função *Trapdoor*
- A técnica de *Hashing* é bastante utilizada no armazenamento de senhas;
- Não é seguro para um banco de dados manter as senhas em um formato que possa ser quebrável;

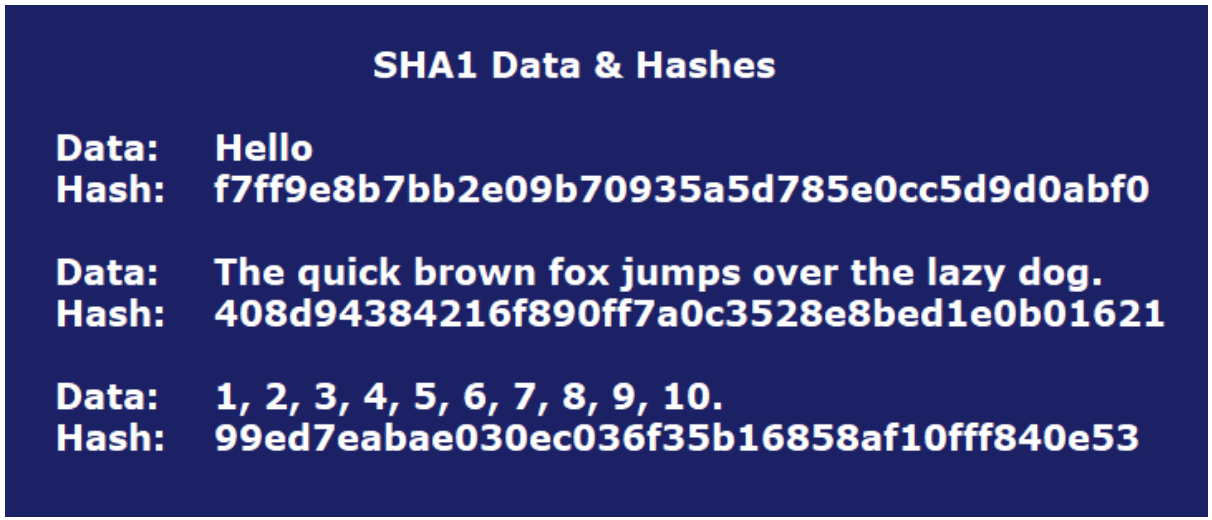


Figura 8: Hashing com SHA1

Hashing

Vantagens, desvantagens e exemplos

- Vantagens:
  - Algoritmo extremamente rápido;
  - Uma forma extremamente segura de armazenar senhas;
- Desvantagens:
  - Podem ocorrer colisões de hashing;
  - Vamos ver agora, que é possível quebrar um algoritmo Hashing com um processador potente;
- Alguns algoritmos *Hashing* famosos são:
  - MD5;
  - SHA-1;
  - SHA-256;

Hashing

Colisões

(a)

(b)

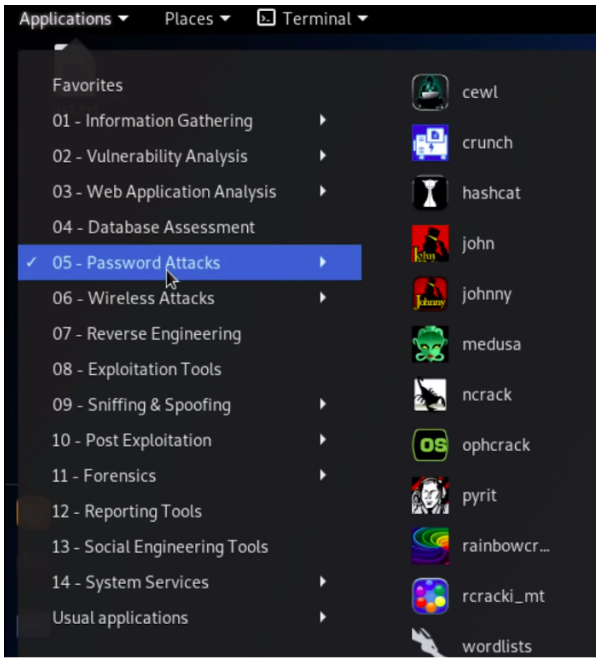
- As imagens (a) e (b) produzem uma colisão quando expostas ao MD5;

Testes de penetração

Kali Linux

- Kali Linux é um sistema operacional que contém um conjunto de ferramentas especiais para realizar testes de penetração;

(a) Kali Linux



(b) Ferramentas

Testes de penetração

HashCat

- HashCat é um programa utilizado para "*recuperação de senhas*";
- Seus modos de ataque são:

0	Straight
1	Combination
3	Brute-force
6	Hybrid Wordlist + Mask
7	Hybrid Mask + Wordlist

HashCat

Dictionary Attack

- Usando o *attack mode 0* podemos realizar um *Dictionary Attack*;
- Esse ataque lê linha por linha de um arquivo *.txt* e tenta as senhas possíveis;
- O arquivo rockyou.txt tem as 14 milhões de senhas mais comuns;
- Exemplo de ataque:

```
hashcat -a 0 -m 0 -o cracked.txt target_hashes.txt rockyou.txt
```

HashCat

Combination

- O *attack mode 1* permite criar um dicionário para realizar um *Combination attack*;
- Nesse ataque, as palavras de *dict1.txt* e *dict2.txt* são combinadas para criar um novo dicionário que pode ser usado;
- Exemplo de ataque:

```
hashcat -a 1 -m 0 -o cracked.txt dict1.txt dict2.txt
```

HashCat

Brute-force

- O *attack mode 3* permite fazer um ataque de força bruta;
- O ataque abaixo, tenta todas as palavras com 8 letras minúsculas: [2]

```
hashcat -a 3 -m 0 <hash> ?l?l?l?l?l?l?l?l
```

- O output seria “password”.

[2] <hash> = 5f4dcc3b5aa765d61d8327deb882cf99

Conclusão

- Nesse seminário vimos que a criptografia já é uma técnica conhecida a milhares de anos;
- A criptografia está presente na maioria das trocas de informações que temos utilizando um computador;
- Existem dois tipos principais: criptografia de chave simétrica ou assimétrica;
  - A criptografia de chave simétrica é mais rápida e simples;
  - Enquanto a de chave assimétrica é mais segura e complexa;
- Existe também uma técnica de Hashing, que é bastante utilizada para armazenar informações sem necessariamente possuir acesso a elas;
- Existem diversos programas criados para tentar quebrar a segurança, por isso é sempre recomendável ter uma senha complexa.

Referências Bibliográficas

Youtube

- Numberphile - 158,962,555,217,826,360,000
- Numberphile - Flaw in the Enigma Code
- Computerphile - Turing's Enigma Problem (Part 1)
- Computerphile - Turing's Enigma Problem (Part 2)
- Numberphile - Encryption and huge numbers
- Thanosmath - Criptografia (1)
- Thanosmath - Criptografia (2)
- Computerphile - Key Exchange Problems

Referências Bibliográficas

Youtube

- Numberphile - RSA-129
- Computerphile - Secret Key Exchange (Diffie-Hellman)
- Computerphile - Public Key Cryptography
- Seytonic - Kali Password Attacks
- Computerphile - Password Cracking
- Computerphile - How to Choose a Password
- Computerphile - How NOT to Store Passwords!

Referências Bibliográficas

Outros

- Wikipedia - History of cryptography
- Brilliant.org - Public Key Cryptography
- Brilliant.org - Symmetric Ciphers
- Brilliant.org - RSA Encription
- Wikipedia - Cryptographic hash function
- HashCat wiki
- Introduction to Algorithms, 3rd Edition, Thomas H. Cohen