

Segurança da Informação– GBC083

Prof. Rodrigo Sanches Miani – FACOM/UFU

Tópicos

Ataques aos sistemas criptográficos

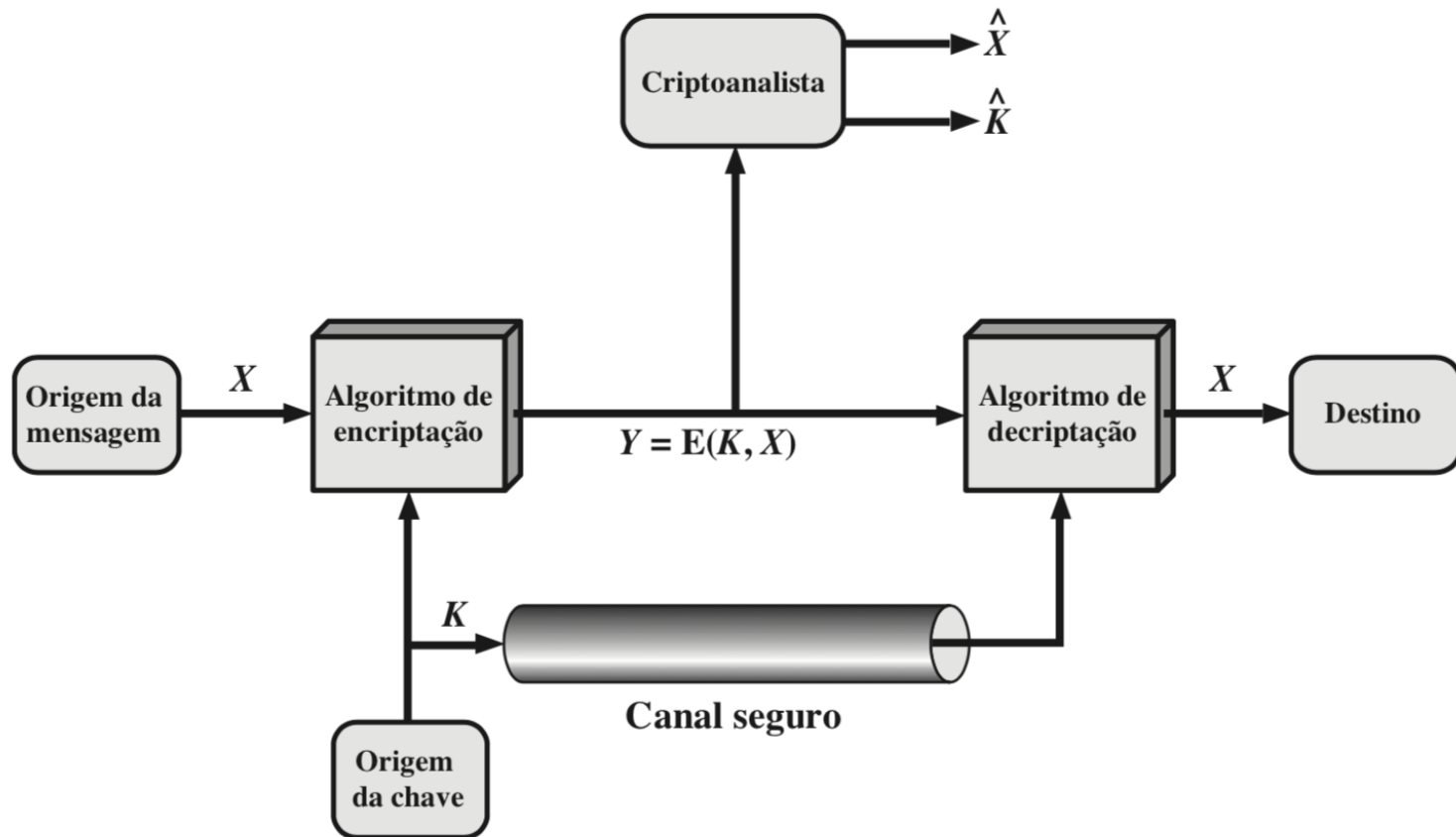
1. Criptoanálise
2. Força-bruta



Ataques aos sistemas criptográficos

Segurança da Informação– GBC083

Visão geral da criptografia



Visão geral da criptografia

Pergunta 1: qual é o principal objetivo em atacar um sistema de criptografia?



Visão geral da criptografia

Pergunta 1: qual é o principal objetivo ao atacar um sistema de criptografia?

Recuperar a chave!



Visão geral da criptografia

Pergunta 2: quais técnicas poderiam ser usadas para recuperar a chave?



Ataques aos sistemas de criptografia

Existem duas técnicas:

1. **Criptoanálise** – estudar a natureza do algoritmo, conhecer características do texto claro ou até obter amostras de pares de texto claro-cifrado;
2. **Ataque por força bruta** – testar todas as chaves possíveis em um texto cifrado.



Criptoanálise

Segurança da Informação– GBC083

Relembrando...

Criptanálise consiste no estudo das técnicas para decifrar uma mensagem sem conhecer o processo usado para cifrá-la.

A seguir, veremos algumas estratégias usadas pelos criptoanalistas.



Ataques aos sistemas de criptografia - Criptoanálise

- ▶ O cenário mais difícil para o criptoanalista é quando a única informação disponível é apenas o texto cifrado;
- ▶ Neste caso, o atacante precisa ter uma ideia geral do tipo de texto claro (texto em inglês, arquivo .exe, código fonte python...) para executar testes mais específicos;
- ▶ Consequentemente, esse é o melhor caso possível para os operadores do sistema de criptografia (remetente e destinatário).



Ataques aos sistemas de criptografia - Criptoanálise

Porém, outras situações podem ocorrer...

- ▶ O atacante pode ser capaz de capturar uma ou mais mensagens de texto claro, além do texto cifrado correspondente;
- ▶ O atacante pode saber que certos padrões de texto claro aparecerão em uma mensagem (arquivo *jpeg* sempre começa com o mesmo padrão de *caracteres*);
- ▶ Isso é chamado de ***ataque de texto claro conhecido***.



Ataque de texto claro conhecido - Exemplo

- ▶ Alice e Bob conversando usando uma ferramenta parecida com WhatsApp.
- ▶ Trudy quer ler as conversas entre eles...
- ▶ Trudy sabe que todo dia de manhã Alice envia uma foto com mensagens de “Bom dia” para o Bob;
- ▶ Caso Trudy consiga coletar tais mensagens, algum tipo de associação pode ser feita entre o texto cifrado coletado e o texto claro conhecido (foto).



Ataques aos sistemas de criptografia - Criptoanálise

Uma outra situação, que pode melhorar a vida do atacante, é a seguinte:

- ▶ Suponha que o atacante, de alguma forma, seja capaz de fazer o emissor inserir no sistema criptográfico uma mensagem escolhida por ele;
- ▶ Tais mensagens poderão revelar a estrutura da chave;
- ▶ Isso é chamado de ***ataque de texto claro escolhido***.



Ataque de texto claro escolhido - Exemplo

- ▶ Alice e Bob conversando usando uma ferramenta parecida com WhatsApp.
- ▶ Trudy quer ler as conversas entre eles...
- ▶ Trudy instiga Alice a enviar alguma mensagem específica para o Bob (fofoca, repasse de mensagem...);
- ▶ Caso Trudy consiga coletar as respectivas mensagens cifradas, agora ela possuirá pares de textos claros e cifrados escolhidos.



Ataques aos sistemas de criptografia - Criptoanálise

- ▶ As análises anteriores mostram que os sistemas criptográficos possuem diferentes níveis de segurança...
- ▶ Veremos a seguir como classificar tais níveis.



Ataques aos sistemas de criptografia - Criptoanálise

Definição I:

- ▶ *um esquema de criptografia é **incondicionalmente seguro** se o texto cifrado gerado por ele **não tiver informação suficiente** para determinar o texto claro correspondente, não importa quanto texto cifrado esteja à disposição do atacante.*



Ataques aos sistemas de criptografia - Criptoanálise

Definição 2:


- ▶ *um esquema de criptografia é considerado **computacionalmente seguro** se **um** dos critérios a seguir for atendido:*
 - ▶ i) O **custo** para quebrar a cifra ultrapassa o **valor** da informação cifrada;
 - ▶ ii) O **tempo** exigido para quebrar a cifra supera o **tempo de vida útil** da informação;



Ataques aos sistemas de criptografia - Criptoanálise

- ▶ Na prática, os algoritmos modernos de criptografia trabalham com a ideia de **computacionalmente seguro**;
- ▶ Veremos que **não** existem algoritmos de criptografia práticos **incondicionalmente seguros**.
 - ▶ Veremos que o OTP não é razoável na prática.





Força-bruta



Segurança da Informação– GBC083

Ataques aos sistemas de criptografia – Força bruta

- ▶ Envolve a tentativa de cada chave possível até que seja obtida uma tradução inteligível de texto cifrado para texto claro;
- ▶ Em média, **metade** de todas as chaves possíveis precisa ser experimentada para se obter sucesso*.
- ▶ Um outro problema surge... Como o atacante sabe que acertou a chave?
- ▶ **Esse resultado decorre do fato de que, assumindo uma distribuição uniforme das chaves e uma busca aleatória ou sequencial, a chave correta será encontrada, em média, na metade do espaço de busca.*



Ataques aos sistemas de criptografia – Força bruta

- ▶ Além de testar as chaves, o atacante precisa reconhecer o texto claro!
 - ▶ Se a mensagem em claro for um texto em português/inglês..., ok!
 - ▶ E se a mensagem foi compactada antes da cifragem?
 - ▶ E se a mensagem for um arquivo binário?



Ataques aos sistemas de criptografia – Força bruta

- ▶ $2^{128/2} = 2^{127}$ - possibilidades para o caso de um AES-128 bits (um dos algoritmos padrão no mercado).
- ▶ <https://www.top500.org/lists/top500/2024/11/>
- ▶ Supercomputador Fugaku - $4.42 * 10^{17}$ FLOPS/s
- ▶ Metade do espaço de chaves do **AES-128** - $2^{127} = 1.7 * 10^{38}$
- ▶ Quanto tempo o supercomputador Fugaku levaria para fazer uma busca exaustiva (ataque de força-bruta) no AES-128?
- ▶ Seria algo factível? O que vocês acham?



Ataques aos sistemas de criptografia – Força bruta

- ▶ $2^{128/2} = 2^{127}$ - possibilidades para o caso de um AES-128 bits (um dos algoritmos padrão no mercado).
- ▶ <https://www.top500.org/lists/top500/2020/11/>
- ▶ Supercomputador Fugaku - $4.42 * 10^{17}$ FLOPS/s
- ▶ Metade do espaço de chaves do **AES-128** - $2^{127} = 1.7 * 10^{38}$

$$4.42 * 10^{17} - \text{Is}$$

$$1.7 * 10^{38} - x$$

$$4.42 * 10^{17}x = 1.7 * 10^{38}$$

$$x = 2.6 * 10^{21} \text{ segundos}$$

$$1 \text{ ano} - 3,154 * 10^7 \text{ segundos}$$

$$x \text{ anos} - 2.6 * 10^{21}$$

$$3,154 * 10^7 x = 2.6 * 10^{21}$$

$$x = 0,82 * 10^{14} \text{ ou } 8,2 * 10^{13} \text{ anos}$$



Roteiro de Estudos

1. Leitura da seção 2.1 “Criptografia e segurança de redes. Princípios e práticas”. William Stallings;
2. Estudo da vídeo-aula referente ao Tópico 3;
3. Vídeo sobre outras aplicações de força-bruta em segurança:

<https://www.youtube.com/watch?v=hkRHQyDirS0>

