**CRIPTOANÁLISE E TIPOS DE ATAQUE

Seção 1.4 – Segurança de Dados, criptografia em rede de computadores,
 Prof. Routo Terada, Professor da USP.**

Quando se analisa a segurança de um algoritmo criptográfico, deve-se especificar que tipo de ataque está sendo considerado. Os objetivos do criptoanalista Carlos são:

1. **quebrar um texto ilegível y interceptado**, ou seja, dado o texto ilegível y conhecer o correspondente texto legível x;
2. **quebrar a chave K**.

Outra terminologia para o assunto, **é usar os termos “texto claro” em relação à “texto legível” e “texto cifrado” ao invés de “texto ilegível”.**

1. **TIPOS DE ATAQUES**

Os tipos de ataques para conseguir (a), em ordem decrescente de insegurança são:

1. ***Ataque por só-texto-ilegível*:**  o criptoanalista Carlos tenta adquirir conhecimento útil à quebra, **analisando apenas** **um ou mais textos ilegíveis y**. Ele faz a análise, baseado na freqüência de letras no idioma usado. Esta análise é conhecida como ataque estatístico. Contando-se todas as ocorrências de cada letra em livros em português, armazenados em computador, conclui-se que cada letra aparece nesses livros com uma freqüência mais ou menos fixa. As vogais aparecem com mais freqüência. A vogal **a** é mais freqüente é aparece 13,5%, seguida de **e** com 12,5%, **i** com 6,0%, a letra **o** com 5,5% e **u** com 4,5%.
A ocorrência usual das consoantes também é fixa. Entre as consoantes, a campeã é **p** com 11,5%, seguida por **t** com 9,0%, **s** com 8,0%, **d** com 5,5%, **n** com 4,5%, **c** com 4,1%, **v** com 4,0%, **q** com 3,0%, etc. Na língua inglesa a frequência é outra – a vogal mais freqüente é **e**, seguida por **a**, **o**, **i** e **u**. Se este tipo de ataque for computacionalmente viável, **o algoritmo em questão, conhecido pelo criptoanalista**, é considerado totalmente inseguro e inútil.
2. ***Ataque por texto legível conhecido*:** o criptoanalista Carlos possui e **analisa pares (x,y) de legível e ilegível correspondentes**, formados com a chave secreta K, desconhecida pelo criptoanalista. Neste e nos tipos de ataques a seguir, o criptoanalista conhece o algoritmo (sem conhecer a chave K) e não é necessariamente um mal-intencionado ou intruso: pode ser um especialista que objetiva descobrir se o algoritmo é vulnerável a este tipo de ataque, sendo que o algoritmo fora projetado por outra pessoa, eventualmente.
3. ***Ataque por texto legível escolhido*:** além do suposto no tipo anterior, o criptoanalista Carlos pode **escolher os textos legíveis x e obter os y correspondentes**. Ele escolhe x que apresente alguma característica estrutural que aumente o seu conhecimento do algoritmo e da chave em uso. Com o conhecimento adquirido, ele pode deduzir o legível x correspondente a um ilegível y novo.
4. ***Ataque adaptativo por texto legível escolhido*:**  além do suposto anterior, a escolha de um novo x pelo criptoanalista Carlos, pode depender dos ilegíveis y analisados anteriormente. Desta forma a escolha de um novo x legível é condicionada ao conhecimento já adquirido pela análise dos y já analisados.
5. ***Ataque por texto ilegível escolhido:*** o criptoanalista Carlos escolhe inicialmente o ilegível y e então obtém o legível x correspondente. Supõe-se que o criptoanalista Carlos tenha acesso apenas ao algoritmo de decriptografia (sem ter acesso à chave), e o seu objetivo é, mais tarde, sem ter mais acesso à decriptografia, ser capaz de deduzir um texto legível x correspondente a um ilegível y novo.
6. ***Ataque adaptativo por texto ilegível escolhido:*** além do suposto no tipo de ataque anterior, a escolha de um novo y pelo criptoanalista Carlos pode depender dos ilegíveis y analisados anteriormente. Desta forma, a escolha de um novo texto ilegível y é condicionada ao conhecimento já adquirido pela análise dos ilegíveis y anteriores.

**Para obter (b) e quebrar a chave K:**

1. ***Ataque por força bruta:*** o criptoanalista Carlos conhece o algoritmo criptográfico e usa a decriptografia. Ele envolve **a tentativa de cada chave K possível**, dentro do espaço de chaves possíveis, até que seja obtida a decriptografia de um texto ilegível y para um texto legível x. Na média, metade de todas as chaves possíveis precisa ser experimentada para se conseguir sucesso.
2. **OUTROS TIPOS DE ATAQUES**

Os ataques a seguir podem ser compostos com os ataques descritos acima ou entre si:

1. ***Ataque por Chaves Conhecidas:*** o criptoanalista Carlos conhece algumas chaves já usadas em sessões de criptografia sobre algum algoritmo e utiliza o conhecimento dessas chaves para deduzir outras chaves novas de sessão.
2. ***Ataque por Repetição:*** o criptoanalista Carlos captura mensagens, gravando as comunicações legítimas entre Alice e Beto, e depois usa parte da gravação para o seu proveito. Se a parte da gravação não é alterada, o ataque é chamado *passivo*. Caso contrário, é chamado *ativo*.
3. ***Personificação:*** o criptoanalista Carlos simula um outro usuário legítimo. Por exemplo, toma o lugar de Alice sem o Beto notar qualquer diferença.
4. ***Ataque por Dicionário:*** muito usado para deduzir senhas quando o criptoanalista Carlos tem acesso ao arquivo de senhas legítimas criptografadas; Carlos calcula antecipadamente as senhas criptografadas y correspondentes às senhas x mais comuns (senhas muito fracas relativas a dados de pessoas) e compara com os y calculados e armazenados no arquivo de senhas legítimas; se encontrar um y igual no arquivo, ele possuirá a senha x válida correspondente.
5. **ALGORITMOS DE CRIPTOGRAFIA**

**Incondicionalmente seguro:** se o texto cifrado gerado pelo algoritmo não tiver informações suficientes para determinar exclusivamente o texto legível correspondente, não importando quanto texto cifrado esteja à disposição. Não importa quanto tempo o oponente tenha, ou seja, é impossível que ele decriptografar o texto cifrado, simplesmente porque não contém informações suficientes para tal.

**Computacionalmente seguro:** se o algoritmo de criptografia atende a um dos critérios seguintes: (a) Custo para quebrar a cifra é superior ao valor da informação codificada. (b) O tempo para quebrar a cifra é superior ao tempo de vida útil da informação.