ESCOLA
SUPERIOR
DE TECNOLOGIA
E GESTÃO

P.PORTO

Criptografia Aplicada

Criptografia Clássica

Agenda

Criptografia - Conceitos

- Criptografia
  - Do Grego kryptós ("escondido") e gráphein ("escrita")
  - Estudo e aplicação de práticas para esconder informação
- Mensagem original / Texto limpo / Texto em claro
  - Conjunto de símbolos que se pretendem manter confidenciais
- Criptograma
  - Resultado de uma operação de cifra de uma mensagem original

06/03/2024 GJH @ Criptografia Aplicada 2024.02 3

Criptografia Clássica

- Tipos de Cifras Clássicas
  - Cifras de Transposição
    - Baseiam-se na reordenação de (conjuntos de) símbolos da mensagem original de acordo com um determinado algoritmo, ou seja os símbolos da mensagem original são trocados de posição entre si.
    - A sua complexidade pode variar significativamente e envolver a utilização de uma chave que determine o processo de transposição

06/03/2024 GJH @ Criptografia Aplicada 2024.02 6

Criptografia Moderna

- Principio de Kerchoff
  - *A cryptosystem should be secure even if the attacker (Oscar) knows all details about the system, with the exception of the secret key. In particular, the system should be secure when the attacker knows the encryption and decryption algorithms.*
  - Nos primórdios da criptografia, considerava-se que a segurança deveria ser mantida através do obscurantismo, mantendo a confidencialidade dos algoritmos utilizados, com várias desvantagens:
    - Ao reduzir o número de pessoas que conheciam o algoritmo, limitava-se também o número de pessoas que poderia identificar os seus pontos fracos
    - A presunção de que o algoritmo é desconhecido de potenciais atacantes reduz o incentivo para procurar elevados níveis de segurança
  - Assim, com a criptografia moderna ganhou proeminência a corrente de opinião inerente ao princípio de Kerchoff, segundo o qual os algoritmos devem ser públicos e apenas as chaves secretas

06/03/2024 GJH @ Criptografia Aplicada 2024.02 19

Aula Teórico-Prática

Descodifique as seguintes mensagens (26 caract.)

- Exercício 1 (ROT4)
  a) IWXK
- Exercício 2 (ROT7)
  a) Lzjvsh Zbwlypvy kl Aljuvsvnph l Nlzahv
- Exercício 3 (ROT13)
  a) Yvprapvnghen rz Frthenaçn Vasbezágvpn rz Erqrf qr Pbzchgnqberf - Pevcgbtensvn Ncyvpnqn - Qbvf zvy r ivagr r dhngeb - Qbvf zvy r ivagr r pvapb

21/02/2024 GJH @ Criptografia Aplicada 2025.02 21

Criptografia - Conceitos

- Criptografia
  - Do Grego kryptós ("escondido“) e gráphein (“escrita“)
  - Estudo e aplicação de práticas para esconder informação
- Mensagem original / Texto limpo / Texto em claro
  - Conjunto de símbolos que se pretendem manter confidenciais
- Criptograma
  - Resultado de uma operação de cifra de uma mensagem original

Criptografia - Conceitos

- Criptoanálise
  - Estudo e aplicação de métodos para quebrar métodos criptográficos
- Criptoanálise Diferencial
  - Baseia-se na análise das diferenças dos criptogramas (e respetivos cálculos intermédios) gerados para conjuntos de mensagens originais, no sentido de descobrir informação que permita quebrar o método utilizado.
    Genericamente, é o estudo de como as diferenças na mensagem original condicionam a diferença no resultado/criptograma
- Criptoanálise Linear
  - Baseia-se na tentativa de encontrar equações que, a partir de determinados bits de entrada/saída, permitam obter o valor (total ou parcial) da chave
  - Composta por duas partes:
    - Construção de equações lineares que permitam relacionar a mensagem original, o criptograma e chave
    - Derivação dos bits da chave através de equações lineares

Criptografia - Conceitos

- Criptografia Clássica vs. Moderna
  - Inicialmente, as técnicas criptográficas foram desenvolvidas essencialmente com fins militares e diplomáticos, sendo usualmente conhecidas como criptografia clássica
  - Os avanços graduais dos sistemas digitais e de computação possibilitaram o desenvolvimento de técnicas criptográficas cada vez mais avançadas e complexas, fortemente alicerçadas em funções matemáticas, a que vulgarmente se chama criptografia moderna

Criptografia Clássica

- Tipos de Cifras Clássicas
  - Cifras de Transposição
    - Baseiam-se na reordenação de (conjuntos de) símbolos da mensagem original de acordo com um determinado algoritmo, ou seja os símbolos da mensagem original são trocados de posição entre si.
    - A sua complexidade pode variar significativamente e envolver a utilização de uma chave que determine o processo de transposição

Criptografia Clássica

- Cifras de Transposição (exemplos)
  - Scytale (of Sparta): Tubo ou pedaço de madeira onde se enrolava uma fita com onde era escrita a mensagem original. O destinatário deve utilizar um tubo do mesmo diâmetro para descodificar a mensagem.

Criptografia Clássica

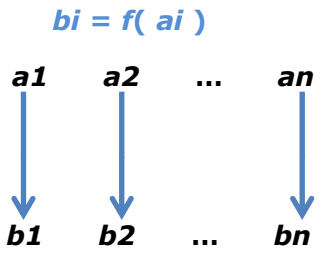
- Cifras de Transposição (exemplos)
  - Guerra Civil Americana
    - Dada a espionagem das linhas de telégrafo por parte das forças inimigas, a utilização de criptografia era vital para assegurar a confidencialidade da comunicação

Message: JAM**ESB**ONDNEEDSBACKUP
Code: J**E**ONDAUA**S**NESCPM**B**DEBK

J	**E**	O	N	D	A	U
A	**S**	N	E	S	C	P
M	**B**	D	E	B	K	

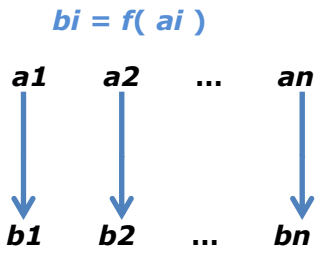
Criptografia Clássica

- Tipos de Cifras Clássicas
  - Cifras de Substituição
    - Baseiam-se na substituição/transformação de cada um dos símbolos da mensagem original, de acordo com um determinado algoritmo
    - Cifras Mono alfabéticas (Puras)
      - Independentemente da sua posição na mensagem original, cada símbolo é cifrado individualmente e mapeado sempre para um mesmo símbolo na mensagem cifrada

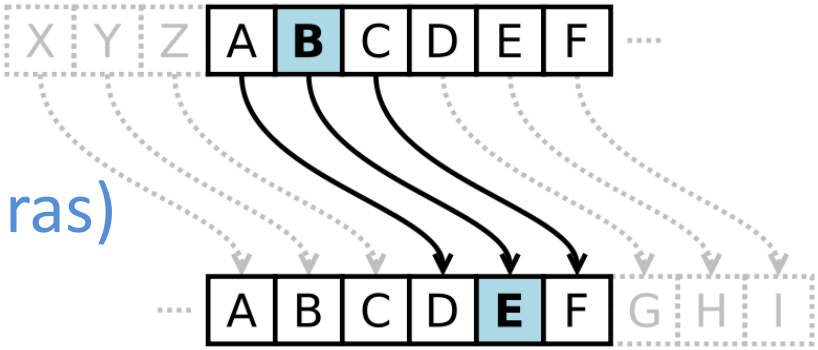


Criptografia Clássica

- Cifras de Substituição:
  - Cifras Mono alfabéticas (Puras)
    - Vantagens:
      - Simplicidade de utilização/implementação
    - Desvantagens:
      - Facilmente atacável por análise de frequência, dada a ocorrência mais frequente de determinado tipo de símbolos (por exemplo, vogais)
      - Facilmente atacável por força bruta, dado o reduzido número de soluções possíveis (que corresponde ao número de caracteres do alfabeto utilizado)



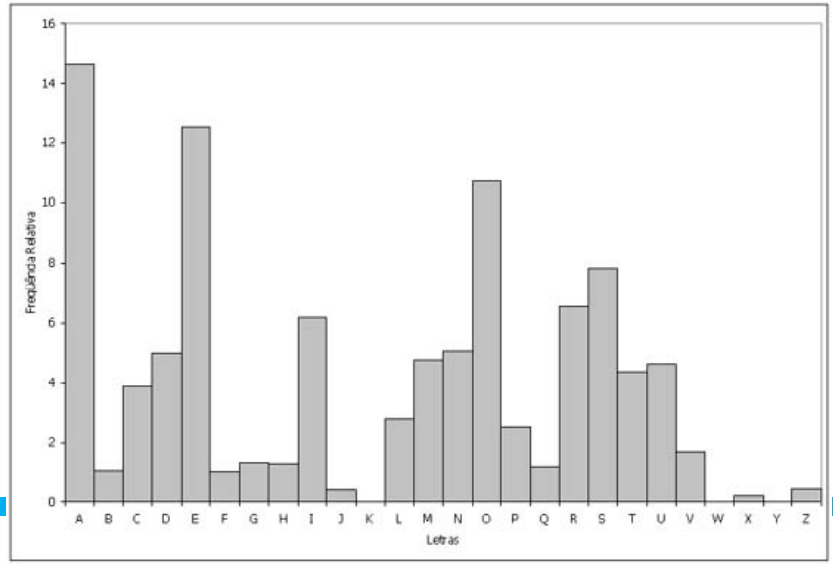
Criptografia Clássica

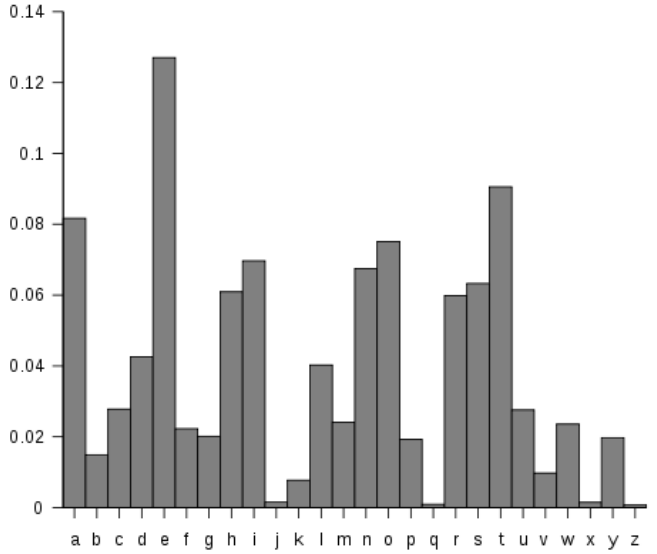


- Cifras de Substituição:
  - Cifras Mono alfabéticas (Puras)
    - Exemplo: Cifra de César
      - Criada por Júlio César para assegurar confidencialidade das mensagens escritas trocadas com os seus generais e enviadas através de mensageiros, que podiam ser intercetados por tropas inimigas
      - É uma cifra de substituição muito simples e baseava-se em deslocar cada letra 3 posições para a direita, ficando conhecida como ROT3
      - Ao atingir o fim do alfabeto, deveria continuar-se a partir do início

Criptografia Clássica

- Análise de Frequência
  - Método utilizado para decifrar mensagens codificadas por meio da análise, nos criptogramas, de padrões que se repetem. A repetição pode indicar a ocorrência de letras ou de palavras comuns, como preposições ("de", "da"), pronomes, ("não", "sim"), etc. O método consiste em primeiro calcular a frequência das letras que aparecem no criptograma e de seguida associar-lhe letras da mensagem original.





Criptografia Clássica

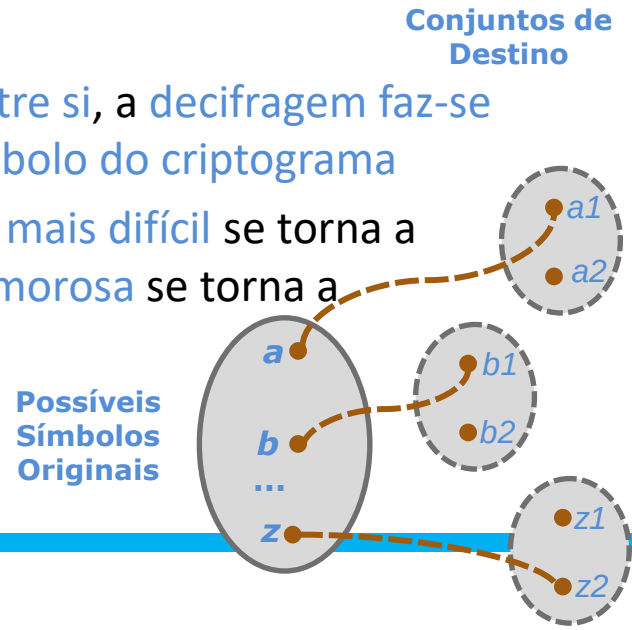
- Ataques por Força Bruta
  - Tipo de ataque mais básico
  - Ataque criptoanalítico que, teoricamente, pode ser utilizado contra quaisquer dados criptografados.
  - Consiste na verificação repetitiva, sistemática e exaustiva de todas as combinações possíveis, até que a chave correta seja encontrada.
  - O tamanho da chave determina o número de combinações, e portanto, a exequibilidade do ataque

Criptografia Clássica

- Ataques de dicionário
  - Consiste na tentativa/teste de todas as chaves pré-definidas numa lista (dicionário).
  - Ao contrário de um ataque por força bruta onde são testadas todas as hipoteses, num ataque de dicionário apenas são testadas as possibilidades com maior probabilidade de sucesso.
  - Este tipo de ataque tem um elevado grau de sucesso porque as pessoas têm tendência para escolher chaves (passwords) curtas, comuns e com variações simples
  - São facilmente ultrapassáveis recorrendo a chaves longas (passphrase por exemplo)

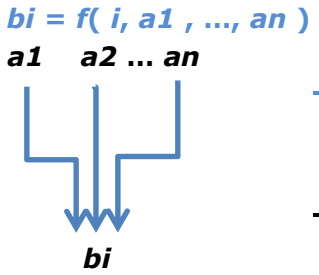
Criptografia Clássica

- Tipos de Cifras Clássicas
  - Cifras de Substituição Homofonica
    - Para cada possível símbolo pertencente à mensagem original é definido um conjunto de possíveis símbolos pelos quais pode ser aleatoriamente substituído
    - Dado que os conjuntos destino são disjuntos entre si, a decifragem faz-se procurando o conjunto a que pertence cada símbolo do criptograma
    - Quanto maiores forem os conjuntos de destino, mais difícil se torna a concretização de ataques de frequência e mais morosa se torna a decifragem



Criptografia Clássica

- Tipos de Cifras Clássicas
  - Cifras de Substituição
    - Cifras Poli alfabéticas (Puras)
      - A transformação aplicada a cada símbolo depende não só de todos os símbolos da mensagem original, como também da posição relativa ocupada pelo símbolo na mensagem original
      - São imunes a análises de frequência, dado que o sucesso no ataque a um símbolo, não facilitaria o ataque dos restantes
      - Dada a sua complexidade computacional, usualmente não podem ser aplicadas de forma purista a mensagens de tamanho realista, dado que isso implicaria ler a totalidade da mesma antes de conseguir cifrar o primeiro símbolo

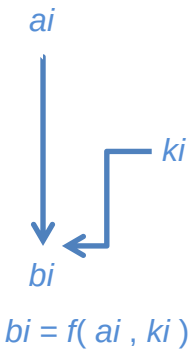


Criptografia Clássica

- (Aproximações às) Cifras Poli Alfabéticas
  - Máquinas Enigma da II Guerra Mundial
    - Por esta altura, a utilização de criptografia já era concretizada através de equipamentos físicos, que:
      - Automatizavam o processo de cifra/decifra
      - Possibilitavam uma maior complexidade e sofisticação dos algoritmos utilizados
      - Utilizava 3 a 6 rotores para implementar uma complexa cifra de substituição
      - A sua quebra foi um marco importante para a vitória aliada

Criptografia Clássica

- (Aproximações às) Cifras Poli Alfabéticas
  - One-Time Pads
    - A transformação aplicada a cada símbolo depende do símbolo da mensagem original e também de um símbolo da chave utilizada
    - Cifra de substituição muito poderosa e impossível de quebrar, caso se garanta:
      - Partilha segura da chave utilizada
      - Que a chave k utilizada é (pelo menos)tão longa quanto a mensagem original
      - Que cada chave utilizada é completamente aleatória e sem relação com as restantes
      - Cada chave é usada apenas uma vez e é destruída após a utilização



$bi = f(ai, ki)$

Criptografia Moderna

- Principio de Kerchoff
  - *A cryptosystem should be secure even if the attacker (Oscar) knows all details about the system, with the exception of the secret key. In particular, the system should be secure when the attacker knows the encryption and decryption algorithms.*
  - Nos primórdios da criptografia, considerava-se que a segurança deveria ser mantida através do obscurantismo, mantendo a confidencialidade dos algoritmos utilizados, com várias desvantagens:
    - Ao reduzir o número de pessoas que conheciam o algoritmo, limitava-se também o número de pessoas que poderia identificar os seus pontos fracos
    - A presunção de que o algoritmo é desconhecido de potenciais atacantes reduz o incentivo para procurar elevados níveis de segurança
  - Assim, com a criptografia moderna ganhou proeminência a corrente de opinião inerente ao princípio de Kerchoff, segundo o qual os algoritmos devem ser públicos e apenas as chaves secretas

Criptografia Aplicada

- Questões?

Aula Teórico-Prática

Descodifique as seguintes mensagens (26 caract.)

- Exercício 1 (ROT4)
    a) IWXK
- Exercício 2 (ROT7)
    a) Lzjvsh Zbwlypvy kl Aljuvsvnph l Nlzahv
- Exercício 3 (ROT13)
    a) Yvprapvnghen rz Frthenaçn Vasbezágvpn rz Erqrf qr Pbzchgnqberf - Pevcgbtensvn Ncyvpnqn - Qbvf zvy r ivagr r dhngeb - Qbvf zvy r ivagr r pvapb

Aula Teórico-Prática

- Exercicio 4

a) Indique o autor do seguinte texto:

ftue xmffqd fqdy ymk tmhq nqqz egssqefqp nk mzouqzf yuf xuzsa--
ftq iadp "tmow" tmp xazs nqqz geqp fa pqeodunq ftq qxmnadmfq
oaxxqsq bdmzwe ftmf yuf efgpqzfe iagxp dqsgxmdxk pqhueq, egot me
oahqduzs ftq payq ftmf ahqdxaawqp ftq omybge iuft dqrxqofuzs
raux. ngf me ftq fydo bqabxq geqp ftq iadp, ftqdq ime eqduage
dqebqof uybxuqp. ituxq eayqazq yustf omxx m oxqhqd oazzqofuaz
nqfiqqz dqxmke m "yqdq tmow," uf iagxp nq gzpqdefaap ftmf, fa
cgmxurk me m tmow, ftq rqmf ygef nq uyngqp iuft uzzahmfuaz,
efkxq, mzp fqotzuomx hudfgaeufk. qhqz ftagst azq yustf
eqxr-pqbdqomfuzsxk emk tq ime "tmowuzs mimk mf ftq ekefqy" (ygot
me mz mjq-iuqxpqd tmowe mf xase), ftq mdfuefdk iuft ituot azq
tmowqp ime dqoaszulqp fa nq oazeupqdmnxq.

Nota: Equacione utilizar a aplicação CrypTool 2

Criptografia Aplicada

Fim!

- Testar aplicação CrypTool para quebra de cifras clássicas