João Miguel Barbosa Gomes

Telmo Rafael Remondes

Relatório Trabalho Prático

18 Junho 2013

Universidade do Minho

Escola de Engenharia

Departamento de Informática



# Índice

Índice 3

Grupo I 4

1.1 Problema 4

1.2 Abordagem 4

1.3 Resultados 5

Grupo II 8

1.4 Problema 8

1.5 Abordagem 8

1.6 Resultados 8

Grupo III 9

1.7 Problema 9

1.8 Abordagem 9

1.9 Resultados 9

Grupo IV 11

1.10 Problema 11

1.11 Abordagem 11

1.12 Resultados 11

Grupo V 12

1.13 Problema 12

1.14 Abordagem 12

1.15 Resultados 12

Grupo VI 13

1.16 Problema 13

1.17 Abordagem 13

1.18 Resultados 13

# Grupo I

## Problema

O problema consiste a criptoanálise de quatro criptogramas obtidos recorrendo a cifras de substituição, shift e Vigenere. O objectivo é descobrir com qual a cifra utilizada para encriptar os criptogramas e obter o texto limpo dos mesmos.

## Abordagem

Visto se saber quais os tipos de cifras usadas para a obtenção dos diferentes criptogramas o primeiro passo passou pela elaboração de programas que fossem capazes de auxiliar à decifração das respectivas cifras. Assim sendo, as capacidades dos diferentes módulos passam pela análise da frequência de caracteres, um algoritmo capaz de dado um valor efetuar o shift em todos os elementos da cifra, um algoritmos que dada uma cifra retornava o espaço entre palavras repetidas na mesma, para além de um programa capaz de fazer a substituição letra a letra de forma muito simples e maleável.

Tendo os algoritmos necessários à decifragem o passo seguinte passou por testar cada um deles nos diferentes criptogramas analisando o resultado que ia sendo obtido de forma a provar que era a cifra que cifrou o criptograma.

Cada para a detecção de cada uma das cifras foram efetuados os seguintes passos:

**Shift:** Primeiramente foi feita uma análise da frequência de caracteres. Tendo estes valores e sabendo-se que se trataria de um texto limpo em inglês ou francês foram comparadas as letras mais observadas nas cifras com as letras mais utilizadas em cada língua. Após a análise feita foi calculado o shift da letra respectiva, tendo o valor do shift foi executado o algoritmo de forma a fazer o shift inverso no criptograma de forma a analisar se o resultado obtido era um texto limpo. Visto ser um criptograma pequeno e visto que a frequência de caracteres podia não bater certo com a frequência de aparecimento no inglês ou francês, foram utilizadas as três letras mais usadas nas línguas e as três letras que mais apareciam no criptograma e calculado o shift para cada uma das possibilidades, juntando todas com todas, de forma a diminuir o risco de erro devido ao tamanho do criptograma.

**Substituição:** Para testar se o criptograma tinha sido cifrado com esta cifra foi feita uma análise da frequência dos caracteres do mesmo. Tendo a frequência de aparecimento dos caracteres do criptograma e a frequência destes nas respectivas línguas, foi feita uma aproximação entre ambos e feita a substituição na cifra. Visto a frequência não coincidir para todos a primeira abordagem foi apenas para um preenchimento inicial da tabela, que foi posteriormente sendo mudada de forma a construir palavras com sentido até obter um texto limpo.

**Vigenere:** De forma a tentar resolver esta cifra foi inicialmente feita uma análise do espaçamento entre os conjuntos de caracteres repetidos e construída uma tabela com os divisores da distancia entre as palavras repetidas. Tendo a tabela preenchida é observado qual o divisor que mais vezes aparece nas palavras repetidas, sendo que este poderá ser o tamanho da chave. Tendo um candidato para tamanho da chave, o criptograma é partido em strings desse mesmo tamanho, tornando o criptograma em pequenas cifras de césar. É feita então a analise de frequência das letras em cada coluna e comparadas com a frequência das letras em cada língua, sendo depois calculada a diferença entre a letra encontrada na coluna e a mais usada na língua, ou seja, o valor do shift. Neste momento é então aplicado o shift encontrado a todas as letras da coluna. Tem de se repetir o processo para cada coluna. Sendo o shift encontrado para cada coluna cada letra da chave, por exemplo se o shift for “1” a letra da chave será “A”.

## Resultados

Os resultados obtidos foram os seguintes:

**Criptograma 1**

**Chave:**

**Cifra:**

**Resultado:**

**Criptograma 2**

**Chave:** crypto

**Cifra:** Vigenere

**Resultado:**

ilearnedhowtocalculatetheamountofpaperneededforaroomwheniwasatschooly

oumultiplythesquarefootageofthewallsbythecubiccontentsofthefloorandceili

ngcombinedanddoubleityouthenallowhalfthetotalforopeningssuchaswindowsand

doorsthenyouallowtheotherhalfformatchingthepatternthenyoudoublethewholet

hingagaintogiveamarginoferrorandthenyouorderthepaper

**Criptograma 3**

**Chave:**

**Cifra:**

**Resultado:**

**Criptograma 4**

**Chave:** theory

**Cifra:** Vigenere

**Resultado:**

igrewupamongslowtalkersmeninparticularwhodroppedwordsafewatatimelikeb

eansinahillandwhenigottominneapoliswherepeopletookalakewobegoncommatomea

ntheendofastoryicouldntspeakawholesentenceincompanyandwasconsiderednotto

obrightsoienrolledinaspeechcoursetaughtbyorvillesandthefounderofreflexiv

erelaxologyaselfhypnotictechniquethatenabledapersontospeakuptothreehundr

edwordsperminute

# Grupo II

## Problema

Foram cifrados vinte textos recorrendo à cifra One-Time-Pad, com aritmética módulo vinte seis. Esta cifra é segura apenas quando usada uma vez, mas nestes vinte criptogramas foi usada a mesma chave para cifrar dois deles. O objectivo é descobrir quais os criptogramas que usam a mesma chave.

## Abordagem

Para tentar resolver o problema foi feito um algoritmo que dados dois criptograma fazia a operação de xor entre eles e devolvia o resultado. O resultado obtido por este algoritmo é o xor das duas mensagens caso tivessem sido cifrados pela mesma chave.

## Resultados

O resultado foi que não foi possível diferenciar quais as mensagens cifradas com a mesma chave. Embora a ideia da forma como se procedia o ataque e das limitações de cifrar duas mensagens com a mesma chave, não foi possível detectar qual a cifra resultante que era constituída pelo xor das duas mensagens.

# Grupo III

## Problema

O problema prende-se com o facto de mostrar que a cifra por blocos Electronic Code Book não consegue esconder os padrões do texto limpo. Para mostrar que isto é verdade, e para observar num caso real essa propriedade do ECB é pedido que seja escolhida uma imagem, retirada apenas a parte que corresponde à imagem propriamente dita, e cifrar esse bloco de informação usando o ECB, e em seguida guarda a imagem novamente. A ideia será verificar que os padrões continuam visíveis mesmo após ser cifrada.

## Abordagem

Para resolver o problema teve em primeiro lugar de se estudar a forma como a imagem era construída. Visto isto, foi ler a área correspondente à imagem, converter para um array de bytes e cifrar, tendo sido cifrado foi apenas necessário voltar a converter para um array de inteiros e reconstruir a imagem.

## Resultados

Como expectável os padrões continuaram visíveis na imagem quando usado o modo ECB. A titulo de experiencia usou se o modo CBC também.



Figura 1 - Normal

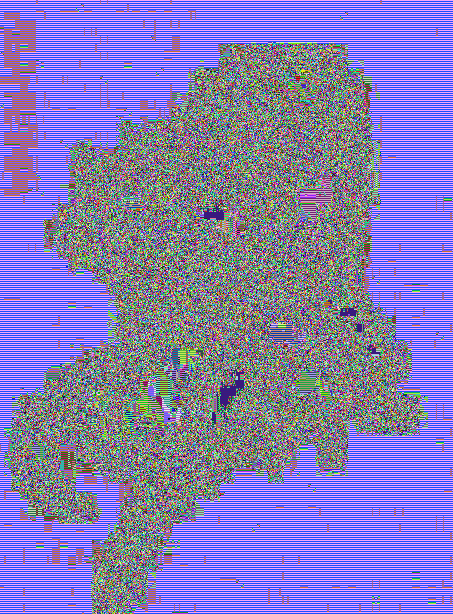


Figura 2 - Modo ECB



Figura 3 - Modo CBC

# Grupo IV

## Problema

## Abordagem

## Resultados

# Grupo V

## Problema

## Abordagem

## Resultados

# Grupo VI

## Problema

## Abordagem

## Resultados