Capítulo 1

Preliminares

1.1 Introdução

Alice deseja enviar uma mensagem a Bob sem que Olga a perceba, no caso desta interceptar a mensagem. Com este objectivo, Alice pode cifrar a mensagem antes de a enviar a Bob. Bob recebe a mensagem e decifra-a. *Critografia* é a ciência que estuda estas duas acções. Se Carla intercepta a mensagem cifrada, pode tentar quebrar a cifra e ler a mensagem. *Criptoanálise* é a ciência em que se estuda métodos ou processos para quebrar cifras. *Criptologia* engloba tanto a Criptografia como a Criptoanálise.

Durante este curso iremos aprender vários sistemas criptográficos, alguns dos quais são correntemente usados nas diversas comunicações de mensagens (militares, espionagem, números de PIN, conversações telefónicas, transacções bancárias, Internet, e-mail, etc.). Ao mesmo tempo, Estudaremos métodos para quebrar certos cifras e a razão pela qual alguns dos sistemas criptográficos são considerados inquebráveis. Iremos também estudar funções de síntese (que são uma espécie de impressão digital), assinaturas e identificação digital e diversos protocolos de segurança. As ferramentas essenciais deste curso serão Teoria dos Números e algumas noções de Álgebra.

1.2 Vocabulário

Mensagem original (ou texto plano) - Mensagem que se pretende tornar secreta, por exemplo OLA;

Mensagem cifrada - A mensagem secreta que se obtém após ter sido

cifrada, por exemplo ROD (usando o sistema criptográfico utilizado por Júlio César);

Emissor - Quem envia a mensagem;

Receptor - Quem recebe a mensagem;

Cifrar - Transformar a mensagem original numa mensagem cifrada;

Decifrar - Transformar a mensagem cifrada na mensagem original;

Cifra - Conjunto de procedimentos e conjunto de símbolos (letras, nomes, sinais, etc) usados para cifrar uma mensagem;

Codificação simples - Transformar a mensagem original em números ou bits[1]. Por exemplo, se fizermos a transformação □ → 0, A→ 1, ..., Z→ 26 então a palavra OLA passava a 15 12 1. Usualmente utiliza-se o código ASCII, que representa cada símbolo por 8 bits (byte): A→ 01000001, B→ 01000010, a→ 01100001, 0 → 00110000, ? → 00111111, etc;

Descodificar - Transformar números ou bits em mensagens;

Monogrâmica (ou monográfica) - Uma cifra que traduz um a um os símbolos do texto original em texto cifrado;

Poligrâmica (ou poligráfica - Uma cifra que traduz vários símbolos do texto original, em grupo e ao mesmo tempo, em texto cifrado;

Cifra de transposição ou permutação - Uma cifra que re-arranja e/ou permuta as letras, símbolos ou bits do texto plano;

Cifra de substituição - Uma cifra que substitui letras, símbolos ou bits por outros sem lhes alterar a ordem;

Sistema criptográfico - Conjunto de procedimentos para cifrar e decifrar uma mensagem;

Chave - Num sistema criptográfico, corresponde a um nome, uma palavra, uma frase, etc, que permite cifrar ou decifrar uma mensagem.

Sistema criptográfico de chave simétrica - Necessita de uma chave secreta partilhada pelo emissor e pelo receptor. O emissor e o receptor têm que concordar com uma chave antes do início da transmissão da mensagem;

Sistema criptográfico de chave pública - Cada utilizador tem uma chave para cifrar que é pública e foi publicada e uma chave para decifrar que é secreta (normalmente só utilizadores autorizados têm a chave secreta);

Assinatura - Processo pelo qual o emissor pode certificar o receptor da sua identidade. Nos sistemas de chave pública este processo evita que utilizadores inimigos enviem mensagens enganosas;

[1] bits é o plural de bit - **bi**nary digi**t**

Criptoanálise - É o processo pelo qual o inimigo (quem não está autorizado a decifrar a mensagem) tenta transformar a mensagem cifrada na mensagem original.

Os processos para cifrar e decifrar devem ser fáceis de aplicar para os utilizadores autorizados mas deve ser difícil um inimigo ou utilizador não autorizado decifrar as mensagens. Teoria dos números é uma excelente fonte de problemas com alguns mecanismos fáceis e alguns mecanismos difíceis, portanto aparenta ser uma óptima área para ser usada em criptologia.

1.3 História

A história da criptografia aparenta ter sido iniciada no antigo Egipto, cerca de 1900 a.C. pelo arquitecto Khnumhotep II, na tempo do faraó Amenemhet II. O escriba de Khnumhotep II substituiu alguns trechos e palavras de documentos importantes por símbolos estranhos de modo a dificultar que ladrões chegassem a tesouros reportados nesses documentos.

Alguns séculos mais tarde aparecem outros métodos de transmitir mensagens de modo secreto, por exemplo na Mesopotâmia, Assíria, China, India e Egipto. Exemplos desses métodos são:

> Tatuagens com mensagens na cabeça de escravos. Infelizmente era preciso esperar o cabelo crescer antes de "enviar" a mensagem. A decifração era feita no barbeiro;
>
> Marcas na madeira de placas de cera. As marcas eram escondidas com cera nova. Para decifrar, bastava derreter a cera;
>
> Mensagens dentro do estômago de animais de caça.

Este tipo de ocultação de mensagens toma o nome de esteganografia e distingue-se da criptografia porque neste caso a mensagem não é alterada e baseia-se no facto de um interceptor não saber da existência da mensagem. Quando se utiliza criptografia, sabe-se que está a ser enviada uma mensagem, mas o seu sentido é obscuro. Como exemplos modernos de esteganografia, temos a ocultação de mensagens em imagens digitais, através da alteração de alguns bits em cada componente da cor e marcas ocultas nas notas bancárias

para evitar a sua falsificação. Apesar da sua aparente semelhança com criptografia, os métodos de esteganografia são muito distintos dos utilizados em criptografia e não serão estudados durante este curso.

Cerca de 600 a.C., os hebreus criaram alguns sistemas criptográficos aquando da escrita do livro de Jeremias, nomeadamente o Atbash, que consiste de uma troca simples entre as letras do hebraico, por ordem inversa.

O primeiro sistema criptográfico de uso militar terá sido o Scytale ou Bastião de Licurgo, utilizado pelo general espartano Pasanius, em 475 a.C.. O scytale consiste em escrever a mensagem numa tira estreita de couro ou pergaminho quando esta está enrolada em torno de um bastião de madeira. A mensagem original é escrita no sentido do comprimento do bastião e, portanto, quando a tira é desenrolada obtém-se a mensagem cifrada. Para voltar a obter a mensagem original, deve-se enrolar outra vez a tira num bastião com o mesmo perímetro e forma. Este é um exemplo de uma cifra de transposição. Esta é ainda a ideia de muitas técnicas populares actuais.

Na India, por volta de 300 a. C., apareceu um livro intitulado Arthasastra, atribuído a Kautilya, onde são referidos os primeiros métodos de criptoanálise. Estes processos são recomendados para diplomatas. O famoso Kama Sutra de Vatsayana, menciona a criptografia nas artes (yogas) 44 e 45, de entre a sua lista de 64 artes e ciências que todos devem saber (Part I, capítulo 3, http://www.sacred-texts.com/sex/kama/index.htm).

Júlio César utilizou uma cifra que consistia em substituir cada letra pela letra que se encontra três posições depois no alfabeto. Este é um exemplo de uma cifra de deslocamento.

No século VIII, al-Khalil, escreveu o livro Kitab al Mu'amma (que significa "O livro das mensagens criptográficas"). Infelizmente este livro desapareceu. al-Khalil decifrou um criptograma bizantino antigo quando supôs, correctamente, que o início do criptograma era "Em nome de Deus". Este método, conhecido como o método da palavra provável, foi usado para ajudar a decifrar mensagens cifradas pelo Enigma, durante a Segunda Guerra Mundial. Cerca de 100 anos depois, al-Kindi, escreveu um outro livro sobre criptografia, ainda existente, intitulado Risalah fi Istikhraj al Mu'amma (Escritos sobre a decifração de mensagens criptográficas). al-Kindi considerou análises estatísticas para quebrar cifras, processo ainda usado na actualidade.

Em 1466, Leon Battista Alberti, escreveu um ensaio, no qual menciona uma cifra em disco, criando a noção de cifra poli-alfabética.

Giovan Batista Belaso inventou, em 1553, um sistema criptográfico poli-alfabético a que actualmente se chama *cifra de Vigenère*, por ter sido fal-

samente atribuído a Blaise de Vigenère durante o século XIX. Este sistema tem uma chave e uma série de diferentes cifras de César e foi considerado indecifrável durante muito tempo, porém é facilmente quebrado utilizando análise estatística. Em 1585, Vigenère criou a noção de auto-chave, processo ainda hoje utilizado, por exemplo no sistema DES.

Durante os séculos XVIII e XIX, assistiu-se à proliferação de *Cameras Escuras*, gabinetes de espionagem, onde se utilizava a criptologia para fins militares e fins civis, nomeadamente para decifrar mensagens diplomáticas. Em Viena, é criada uma das mais eficientes cameras escuras, onde se decifrava cerca de 100 mensagens diplomáticas internacionais, por dia. França, Inglaterra e Alemanha também criam os seus centros de criptoanálise, tendo empregado diversos matemáticos famosos.

Durante a Primeira Guerra Mundial assiste-se a uma proliferação de sistemas criptográficos para usos militares. Como exemplos, temos o Playfair e o ADFGVX.

A cifra inglesa Playfair (guerra dos Boers e Primeira Guerra Mundial) consiste em escrever a palavra chave (que não pode ter letras repetidas) seguida das restantes letras num quadrado cinco por cinco. Se considerarmos a palavra chave *Palmerston*, obtemos

P	A	L	M	E
R	S	T	O	N
B	C	D	F	G
H	IJ	K	Q	U
V	W	X	Y	Z

Para cifrar um par de letras, forma-se um rectângulo do qual as letras são vértices. A mensagem cifrada consiste dos outros dois vértices. Por exemplo, *PI* é cifrado em *AH*. Se duas letras estão na mesma linha (resp. mesma coluna), toma-se as letras seguintes, e. g. *EU* é cifrado em *NZ* e *ME* fica *EP*. Se a mensagem original tiver duas letras iguais consecutivas, coloca-se um *X* a separá-las, e. g. a mensagem *ASSIM* passa a ser *AS XS IM*.

A cifra alemã ADFGVX (Primeira Guerra Mundial), utiliza uma tabela fixa para efectuar uma substituição da mensagem original. Cada letra é transformada no par de letras correspondente à linha e coluna onde a letra original está.

	A	D	F	G	V	X
A	K	Z	W	R	1	F
D	9	B	6	C	L	5
F	K	7	J	P	G	X
G	E	V	Y	3	A	N
V	8	O	D	H	0	2
X	U	4	I	S	T	M

Assim, *ACHTUNG* é primeiro cifrado em *GV DG VG XV XA GX FV*. Esta é a parte da substituição da cifra.

Em seguida, efectua-se um deslocamento, utilizando uma chave sem letras repetidas, neste caso a chave é *DEUTSCH*. Constrói-se uma tabela em que, na primeira linha está a palavra chave, na segunda linha o numeral correspondente à ordem alfabética de cada letra da primeira linha e, nas linhas seguintes é escrita a mensagem que resultou do processo de substituição efectuado anteriormente. A mensagem cifrada é obtida, escrevendo as letras das colunas seguindo a ordem indicada na segunda linha.

D	E	U	T	S	C	H
2	3	7	6	5	1	4
G	V	D	G	V	G	X
V	X	A	G	X	F	V

No nosso exemplo, a mensagem cifrada correspondente à mensagem original *ACHTUNG* é *GF GV VX XV VX GG DA*.

A grande fraqueza da cifra ADFGVX é usar uma tabela fixa para a parte da substituição. A alternância entre substituições e deslocações permite obter cifras bastante seguras, sendo este processo a base do DES (Data Encryption Standard) e do AES (Advanced Encryption Standard).

Após esta guerra começam a aparecer as primeiras máquinas cifrantes que usam rotores mecânicos. Em 1923, Arthur Scherbius, desenvolve o ENIGMA, talvez a mais famosa máquina cifrante. O ENIGMA é utilizado pelos alemães durante a Segunda Guerra Mundial para comunicações com os submarinos e para deslocar as suas tropas. O ataque criptoanalítico ao ENIGMA foi iniciado pelo matemático polaco Marian Rejewski (juntamente com Jerzy Rozycki e Henryk Zygalski), que após a Polónia ter sido invadida conseguiu passar a sua informação para França. Esta informação acabou por chegar a Inglaterra, onde Turing e o seu grupo de criptoanalíticos trabalhavam. Estes conseguiram decifrar o ENIGMA o que permitiu descobrir planos mil-

itares dos alemães e o envio mensagens enganosas para os alemães localizados em França, conseguindo assim facilitar a invasão por Dunquerque. Japão tinha a Máquina Púrpura, cujo sistema foi quebrado por equipa liderada por William Frederick Friedman (criador da palavra criptoanálise). O sistema criptográfico utilizado pelos EUA durante Segunda Guerra Mundial, encontra-se ainda classificado.

Nos anos 60, o Dr. Horst Feistel, liderando um projecto de pesquisa no IBM Watson Research Lab, desenvolve a cifra Lucifer. Em 1974, a IBM apresenta Lucifer ao NBS (National Bureau of Standards), o qual, após algumas alterações, adopta esta cifra como cifra padrão nos EUA, criando assim o DES (Data Encryption Standard). Este sistema foi criticado desde o início por vários investigadores e acabou por ser quebrado, usando força bruta, em 1997.

Whitfield Diffie e Martin Hellman publicam, em 1976, o artigo "New Directions in Cryptography", onde introduzem a ideia de criptografia de chave pública, neste caso baseada no problema do logaritmo discreto, e avançam com a ideia de autenticação utilizando funções de um só sentido (one way functions). Inspirados por aquele artigo, Ronald L. Rivest, Adi Shamir e Leonard M. Adleman, desenvolvem uma cifra de chave pública, que também pode ser usada para assinaturas digitais, baseada no contraste entre a dificuldade de factorizar números grandes e a relativa facilidade de identificar números primos grandes. Este sistema passou a ser conhecido como RSA e foi patenteado. Em 1984, Taher Elgamal desenvolve o sistema ElGamal também utilizando o problema do logaritmo discreto.

Nos anos 90 aparecem diversos sistemas criptográficos em particular o IDEA (International Data Encryption Algorithm) de Xuejia Lai e James Massey, que pretende ser um substituto do DES. A criptografia quântica é introduzida em 1990. O PGP (Pretty Good Privacy) de Phil Zimmermann, desenvolvido em 1991, ainda é um dos programas mais utilizados para proteger a privacidade do e-mail e dos arquivos guardados no computador do utilizador. Nas versões mais recentes do PGP, é utilizado o sistema ElGamal. Em 1997, o NIST solicitou propostas para a substituição do DES. Em 2000, o NIST escolheu o Rijndael (de entre os finalistas estava MARS da IBM, RC6 de RSA Laboratories, Rijndael de Joan Daemen e Vincent Rijmen, Serpent de Anderson, Biham e Knudsen, e o twofish de Bruce Schneier e sua equipa), para ser o novo AES (Advanced Encryption Standard). Só em 2005 é que o NIST (National Institute of Standards and Technology), que substituiu o NBS, publica um plano de transição com a duração de dois anos, para que as

agências governamentais deixassem de utilizar o DES e passassem a utilizar o AES.

Capítulo 3

Criptografia Simétrica

Criptografia é a arte e ciência de enviar mensagens secretas. O emissor usa uma chave para cifrar a mensagem, esta é enviada até ao receptor que usa outra chave para a decifrar. Escrevendo letras e sinais de pontuação como números, podemos assumir que a mensagem a enviar é um inteiro P que é codificado num outro inteiro C. O problema consiste em inventar chaves que tornem impossível ou computacionalmente irrealizável que o inimigo (ou qualquer pessoa que não queiramos que leia a mensagem) decifre a mensagem interceptada. Muitas vezes a criptografia usa chaves secretas que só são conhecidas pelo emissor e pelo receptor. Se o inimigo descobre a chave de cifrar e intercepta a mensagem cifrada, ele pode conseguir descobrir a chave de decifrar e recuperar a mensagem original. Este foi o método que os matemáticos ingleses usaram para decifrar o *Enigma*, usado pelos alemães para comunicar entre si e, em particular, com os submarinos, na segunda guerra mundial.

Neste capítulo iremos estudar alguns exemplos clássicos de criptosistemas.

3.1 Introdução

Normalmente, o primeiro passo para inventar um criptosistema consiste em codificar a mensagem, i. e. transformar a mensagem original em números ou bits. Este processo pode ser efectuado letra a letra, e. g. A$\rightarrow$ 0, ..., Z$\rightarrow$ 25, ou em pares de letras, e. g. dadas duas letras correspondentes a $x, y \in \{0, 1, \ldots, 25\}$, o par de letras irá corresponder ao inteiro

$$26x + y \in \{0, 1, \ldots, 675\}.$$

Por exemplo, o par "EU"corresponde ao número 125. A codificação pode também ser feita a n-uplos de letras, $n \geq 3$, fazendo-se a correspondência: se a letra α_i corresponde ao número x_i então o n-uplo $\alpha_1 \cdots \alpha_n$ corresponde a inteiro

$$26^{n-1}x_1 + \cdots 26x_{n-1} + x_n.$$

Durante este curso, usaremos essencialmente as codificações

1. A$\rightarrow$ 0, ..., Z$\rightarrow$ 25;
2. $\Box \rightarrow 0$, A$\rightarrow 1, \ldots,$ Z$\rightarrow 26$;
3. $\Box \rightarrow 0$, A$\rightarrow 1, \ldots,$ Z$\rightarrow 26, 0 \rightarrow 27, \ldots 9 \rightarrow 36$;
4. O código ASCII.

Definição. Um criptosistema é um quíntuplo $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ que satisfaz as seguintes condições:

1. $\mathcal{P}$ é o conjunto finito dos textos planos possíveis;
2. $\mathcal{C}$ é o conjunto finito dos textos cifrados possíveis;
3. $\mathcal{K}$ é o conjunto finito das chaves;
4. Para cada $K \in \mathcal{K}$ existe uma regra para cifrar $e_K \in \mathcal{E}$ e uma regra para decifrar correspondente $d_K \in \mathcal{D}$, tais que $e_K : \mathcal{P} \longrightarrow \mathcal{C}$, $d_K : \mathcal{C} \longrightarrow \mathcal{P}$ e $d_K(e_K(x)) = x$, para qualquer $x \in \mathcal{P}$.

3.2 Cifra de Substituição

As cifras de Substituição são utilizadas à centenas de anos. Actualmente ainda aparecem em Criptogramas nas revistas recreativas. Como o próprio nome indica, estas cifras consistem em substituir cada letra por uma outra letra. Nestas cifras não é necessário codificar a mensagem primeiro.

Cifra (Substituição)**.** *Seja m um inteiro positivo. Sejam $\mathcal{P} = \mathcal{C} = \mathbb{Z}_m$. O conjunto das chaves $\mathcal{K}$ consiste de todas as permutações dos números $0, 1, \ldots, m-1$. Sejam $x \in \mathcal{P}$ e $y \in \mathcal{C}$. Para cada permutação $\pi \in \mathcal{K}$, definimos*

$$e_\pi(x) = \pi(x)$$

e

$$d_\pi(y) = \pi^{-1}(y),$$

onde π^{-1} *é a permutação inversa de* π.

Estas cifras têm $m!$ chaves possíveis. No caso de $m = 26$, obtemos mais de 4.0×10^{26} chaves, o que torna impraticável a busca exaustiva da chave de um sistema criptográfico deste tipo. Mais tarde veremos como quebrar estes sistemas.

Exercício. *Considere* $m = 26$. *Sabendo que foi utilizada uma cifra de substituição, decifre a seguinte mensagem na língua inglesa.*

MGZVYZLGHCMHJMYXSSFMNHAHYCDLMHA

3.3 Criptoanálise clássica

Suponhamos que se deseja decifrar uma mensagem, mas não se sabe a chave. Para isso usa-se criptoanálise. Diz-se *quebrar o código* ao processo de descobrir como decifrar mensagens num dado criptosistema sem se saber as chaves. Para quebrar um código necessitamos de dois tipos de informação: que tipo de criposistema temos, e quais são as chaves desse criptosistema. Iremos assumir que o tipo de criptosistema a quebrar é conhecido (princípio de Kerckhoff) e iremos só estudar como descobrir as chaves.

Há vários níveis de ataques a um criptosistema, os mais comuns são

Só mensagem cifrada(ciphertext-only): O oponente possui uma mensagem cifrada;

Texto plano conhecido (known plaintext): O oponente possui um texto plano e a mensagem cifrada correspondente;

Texto plano escolhido (chosen plaintext): o oponente obteve acesso temporário à máquina de cifrar. Portanto pode escolher um texto plano e cifrá-lo.

Mensagem cifrada escolhida (chosen ciphertext): O oponente obteve acesso temporário à máquina de decifrar. Portanto pode escolher uma mensagem cifrada e decifrá-la.

Letra	E	T	A	O	I	N	S
Probabilidade	0.127	0.091	0.082	0.075	0.070	0.067	0.063
Letra	H	R	D	L	C	U	M
Probabilidade	0.061	0.060	0.043	0.040	0.028	0.028	0.024
Letra	W	F	G	Y	P	B	V
Probabilidade	0.023	0.022	0.020	0.020	0.019	0.015	0.010
Letra	K	J	X	Q	Z		
Probabilidade	0.008	0.002	0.001	0.001	0.001		

Figura 3.1: Distribuição de Frequências na Língua Inglesa

Letra	A	E	O	S	R	I	N
Probabilidade	0.146	0.126	0.107	0.078	0.065	0.062	0.051
Letra	D	M	T	U	C	L	P
Probabilidade	0.050	0.047	0.047	0.046	0.039	0.028	0.025
Letra	H	G	Q	B	F	V	J
Probabilidade	0.013	0.013	0.012	0.010	0.010	0.009	0.004
Letra	J	X	K	W	Y		
Probabilidade	0.004	0.002	0.001	0.001	0.001		

Figura 3.2: Distribuição de Frequências na Língua Portuguesa

Normalmente, é preferível usar textos planos sem espaços nem pontuação, tornando o criptosistema mais seguro.

Muitas técnicas de criptoanálise utilizam as propriedades estatísticas de uma língua. Nas figuras 3.1 e 3.2 estão representadas as frequências relativas das línguas Inglês e Português, respectivamente. Por vezes temos também de usar as frequências relativas de duas ou três letras consecutivas (digramas e trigramas). Os digramas mais frequentes na língua inglesa são: TH, HE, IN, ER, AN, RE, ED, ON, ES, ST, EN, AT, TO, NT, HA, ND, OU, EA, NG, AS, OR, TI, IS, ET, IT, AR, TE, SE, HI e OF. Os trigramas mais frequentes na língua inglesa são: THE, ING, AND, HER, ERE, ENT, THA, NTH, WAS, ETH, FOR e DTH.

3.4 Criptoanálise da Cifra de Substituição

Vamos complicar um pouco e analisar como se pode quebrar a cifra de substituição. Considere a mensagem cifrada

YIFQFM ZRWQFY VECFMD ZPCVMR ZWNMDZ VEJBTX
CDDUMJ NDIFEF MDZCDM QZKCEY FCJMYR NCWJCS
ZREXCH ZUNMXZ NZUCDR JXYYSM RTMEYI FZWDYV
ZVYFZU MRZCRW NZDZJJ XZWGCH SMRNMD
HNCMFQ CHZJMX JZWIEJ YUCFWD JNZDIR

A seguinte tabela apresenta a análise de frequência desta mensagem cifrada

Letra	A	B	C	D	E	F	G	H	I
Frequência	0	1	15	13	7	11	1	4	5
Letra	J	K	L	M	N	O	P	Q	R
Frequência	11	1	0	16	9	0	1	4	10
Letra	S	T	U	V	W	X	Y	Z	
Frequência	3	2	5	5	8	6	10	20	

Como o Z aparece significativamente mais vezes que qualquer outra letra, podemos conjecturar que $d_K(Z) = e$. As outras letras que aparecem pelo menos de 9 vezes são *M, C, D, F, J, R, Y, N* e será de esperar que estas letras sejam obtidas a partir de *t, a, o, i, n, s, h, r*, mas por termos um texto tão pequeno, as frequências não variam de modo suficiente para nos dar a correspondência correcta.

Nesta altura, é aconselhável considerar digramas, especialmente aqueles que contém a letra Z. Verifica-se que os digramas DZ e ZW aparecem quatro vezes cada, que os digramas NZ e ZU aparecem três vezes cada e que os digramas *RZ, HZ, XZ, FZ, ZR, ZV, ZC, ZD, ZJ* aparecem duas vezes cada. Como ZW aparece quatro vezes, WZ nunca aparece e W não é das letras que mais aparecem, podemos conjecturar que $d_K(W) = d$. Como DZ aparece quatro vezes e ZD aparece duas vezes, podemos esperar que $d_K(D) \in \{r, s, t\}$, mas não conseguimos, de uma maneira clara, prever qual das três possibilidades é a correcta.

Assumindo $d_K(W) = d$, verifica-se que os únicos digramas com W no fim, que aparecem mais que uma vez são ZW e RW. Entre os digramas mais frequentes na língua inglesa, os únicos que terminam em d são ed e nd, donde somos levados a conjecturar que $d_K(R) = n$.

Antes de continuarmos a nossa análise, vejamos quais são os digramas que mais aparecem na mensagem cifrada. Além dos digramas DZ e ZW também MD e MR aparecem quatro vezes cada, e, além de NZ e ZU, também CD, CH, FM, IF e NM aparecem três vezes. Atendendo aos digramas mais frequentes na língua inglesa podemos inferir que $d_K(M) \in \{a, i, n, o, s\}$ e $d_K(R) \in \{n, r, s, t\}$. Mais, como NM e NZ são frequentes, então provavelmente temos $d_K(NM) \in \{ha, hi\}$.

A última afirmação permite-nos conjecturar que $d_K(N) = h$ e $d_K(M) \in \{a, i\}$.

Vejamos como fica a frase se efectuarmos as substituições conjecturadas:

- - - - - -	end - - -	- - - - - -	e - - - - n	edh - - e	- - - - - -
YIFQFM	ZRWQFY	VECFMD	ZPCVMR	ZWNMDZ	VEJBTX
- - - - - -	h - - - - -	- - e - - -	- e - - - -	- - - - - n	h - d - - -
CDDUMJ	NDIFEF	MDZCDM	QZKCEY	FCJMYR	NCWJCS
en - - - -	e - h - - e	he - - - n	- - - - - -	n - - - - -	- ed - - -
ZREXCH	ZUNMXZ	NZUCDR	JXYYSM	RTMEYI	FZWDYV
e - - - e -	- ne - nd	he - e - -	- ed - - -	- - nh - -	
ZVYFZU	MRZCRW	NZDZJJ	XZWGCH	SMRNMD	
- h - - - -	- - e - - -	- ed - - -	- - - - d -	- he - - n	
HNCMFQ	CHZJMX	JZWIEJ	YUCFWD	JNZDIR	

A sequência ne - nd sugere que devemos substituir C por a o que implica que $d_K(M) = i$. Donde

- - - - - i	end - - -	- - a - i -	e - a - in	edhi - e	- - - - - -
YIFQFM	ZRWQFY	VECFMD	ZPCVMR	ZWNMDZ	VEJBTX
a - - - i -	h - - - - -	i - ea - i	- e - a - -	- a - i - n	had - a -
CDDUMJ	NDIFEF	MDZCDM	QZKCEY	FCJMYR	NCWJCS
en - - a -	e - hi - e	he - a - n	- - - - - i	n - i - - -	- ed - - -
ZREXCH	ZUNMXZ	NZUCDR	JXYYSM	RTMEYI	FZWDYV
e - - - e -	ineand	he - e - -	- ed - a -	- inhi -	
ZVYFZU	MRZCRW	NZDZJJ	XZWGCH	SMRNMD	
- hai - -	a - e - i -	- ed - - -	- - a - d -	- he - - n	
HNCMFQ	CHZJMX	JZWIEJ	YUCFWD	JNZDIR	

Das vogais mais frequentes só nos falta determinar a letra que corresponde a *o*. Sabemos que esta letra é muito comum, portanto será aceitável supor que é uma das letras *D, F, J, Y*. Mas *D, F, J* são facilmente eliminadas senão provocavam sequências de muitas vogais no texto plano. Conjecturamos então que $d_K(Y) = o$. Quando se faz esta substituição, obtém-se as sequências *a-ion* o que sugere a terminação *ation* muito comum em inglês. Assim, $d_K(J) = t$.

o - - - - i	end - - o	- - a - i -	e - a - in	edhi - e	- - t - - -
YIFQFM	ZRWQFY	VECFMD	ZPCVMR	ZWNMDZ	VEJBTX
a - - - it	h - - - - -	i - ea - i	- e - a - o	- ation	hadta -
CDDUMJ	NDIFEF	MDZCDM	QZKCEY	FCJMYR	NCWJCS
en - - a -	e - hi - e	he - a - n	t - oo - i	n - i - o -	- ed - o -
ZREXCH	ZUNMXZ	NZUCDR	JXYYSM	RTMEYI	FZWDYV
e - o - e -	ineand	he - ett	- ed - a -	- inhi -	
ZVYFZU	MRZCRW	NZDZJJ	XZWGCH	SMRNMD	
- hai - -	a - eti -	ted - - t	o - a - d -	the - - n	
HNCMFQ	CHZJMX	JZWIEJ	YUCFWD	JNZDIR	

Já tínhamos reparado que $d_K(D) \in \{r, s, t\}$. Atendendo à sequência *d-the*, faz sentido considerar que $d_K(D) = s$. Das letras mais frequentes só nos sobram F e r. Donde $d_K(F) = r$.

o - r - ri	end - ro	- - aris	e - a - in	edhise	- - t - - -
YIFQFM	ZRWQFY	VECFMD	ZPCVMR	ZWNMDZ	VEJBTX
ass - it	hs - r - r	iseasi	- e - a - o	ration	hadta -
CDDUMJ	NDIFEF	MDZCDM	QZKCEY	FCJMYR	NCWJCS
en - - a -	e - hi - e	he - asn	t - oo - i	n - i - o -	redso -
ZREXCH	ZUNMXZ	NZUCDR	JXYYSM	RTMEYI	FZWDYV
e - ore -	ineand	hesett	- ed - a -	- inhis	
ZVYFZU	MRZCRW	NZDZJJ	XZWGCH	SMRNMD	
- hair -	a - eti -	ted - - t	o - a - ds	thes - n	
HNCMFQ	CHZJMX	JZWIEJ	YUCFWD	JNZDIR	

Agora, facilmente se obtém

> Our friend from Paris examined his empty glass with surprise, as if evaporation had taken place while he wasn't looking. I poured some more wine and he settled back in his chair, face tilted up towards the sun

3.5 Cifra de Deslocamento

Nesta subsecção, apresentamos as cifras de deslocamento, da qual o sistema criptográfico utilizado por Júlio César é um exemplo. A base desta cifra, assim como de outras cifras que estudaremos posteriormente, é a aritmética modular.

Definição. Sejam a e b inteiros e n um inteiro positivo. Se $n \mid (a-b)$, dizemos que a é *congruente* com b e escrevemos

$$a \equiv b \mod n$$

Cifra (Deslocamento)**.** *Seja m um inteiro positivo. Sejam $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_m$. Para $0 \leq K \leq m-1$, $x \in \mathcal{P}$ e $y \in \mathcal{C}$ definimos*

$$e_K(x) \equiv x + K \mod m$$

e

$$d_K(y) \equiv y - K \mod m$$

A cifra de César é uma cifra de deslocamento, com $K = 3$ e $m = 23$. O ROT-13, actualmente utilizado online, em newsgroups e usenet, para ocultar mensagens ofensivas, respostas a puzzles, etc., é outro exemplo de uma cifra de deslocamento, neste caso com $K = 13$ e $m = 26$. Note-se que, neste caso $e_K(e_K(x)) = x$.

As cifras de deslocamento são exemplos de cifras de substituição.

As cifras de deslocamento são muito inseguras, porque há somente m chaves possíveis, e m é normalmente muito pequeno. Uma busca exaustiva da chave quebra rapidamente um destes sistemas criptográficos.

Exercício. *A seguinte mensagem foi cifrada com uma cifra de deslocação com $m = 27$. Decifre-a.*

OCUAE SCMRUMLQLDQSFCMZOM

3.6 Algoritmo de Euclides e inversos $\bmod n$

Antes de vermos mais sistemas criptográficos, necessitamos de alguns resultados elementares da Teoria dos Números.

Definição. Sejam a e b dois inteiros tais que pelo menos um deles é não nulo. Chamamos *máximo divisor comum* ao maior elemento do conjunto dos divisores comuns de a e b e denotamos este elemento por (a, b).

Sejam a e b dois inteiros positivos. Pelo algoritmo da divisão, existem dois inteiros q_0 e r_0, tais que

$$a = q_0 b + r_0, \quad \text{com} \quad 0 \leq r_0 < b$$

Se $r_0 \neq 0$ podemos utilizar o algoritmo da divisão para os inteiros b por r_0. Então existem q_1 e r_1 tais que

$$b = q_1 r_0 + r_1, \quad \text{com} \quad 0 \leq r_1 < r_0$$

Procedendo desta forma obtemos uma sequência de inteiros não negativos $r_0, r_1, \ldots, r_n$, tais que $r_0 > r_1 > \cdots > r_n \geq 0$. Note que este processo tem de terminar ao fim de um número finito de passos e que o último resto, que denotamos por r_{k+1}, é nulo.

Teorema 3.1. *Se a e b são dois inteiros positivos e r_k é o último resto não nulo obtido pelo algoritmo de Euclides, então $r_k = (a, b)$. Mais, o algoritmo de Euclides permite encontrar inteiros u e v tais que*

$$au + bv = (a, b)$$

Demonstração: O algoritmo de Euclides pode ser esquematizado pelo seguinte sistema de equações:

$$\begin{cases} a = bq_0 + r_0 \\ b = r_0 q_1 + r_1 \\ r_0 = r_1 q_2 + r_2 \\ \vdots \\ r_{k-2} = r_{k-1} q_k + r_k \\ r_{k-1} = r_k q_{k+1} \end{cases} \tag{3.1}$$

Seja $d = (a, b)$. Vamos provar por indução que $d|r_i$ e $d|r_{i+1}$, para todo o $0 \leq i \leq k-1$. Como $d|a$ e $d|b$, temos $d|(a - bq_0)$, i.e., $d|r_0$. Como $d|b$ e $d|r_0$ então $d|(b - r_0 q_1) = r_1$. Agora, suponhamos que $d|r_i$ e $d|r_{i+1}$, queremos provar que $d|r_{i+1}$ e $d|r_{i+2}$. Usando a hipótese de indução, obtemos que $d|(r_i - r_{i+1} q_{i+2})$. Mas $r_i - r_{i+1} q_{i+2} = r_{i+2}$. Portanto $d|r_{i+2}$.

Acabámos de provar que $d|r_i$ para todo $0 \leq i \leq k$. Em particular, $d|r_k$. Como $d, r_k > 0$, temos $d \leq r_k$.

Reciprocamente, a última equação em (3.1) e o facto de $r_k \neq 0$, diz-nos que $r_k|r_{k-1}$. Usando a penúltima equação, obtemos $r_k|r_{k-2}$. Por indução, concluímos que $r_k|r_i$, para qualquer $0 \leq i \leq k$. Usando a segunda equação, temos $r_k|b$ e usando a primeira, $r_k|a$. Logo, $r_k|d$. Portanto, $r_k = d$.

Agora, provamos a segunda parte do teorema. Seja $r_{-2} = a$ e $r_{-1} = b$. Sabemos que

$$r_i = r_{i-2} - r_{i-1} q_i, \tag{3.2}$$

para qualquer $0 \leq i \leq k$. Vamos provar por indução que, para qualquer $0 \leq i \leq k$, existem inteiros u_i e v_i tais que $r_i = u_i a + v_i b$. Como $r_0 = a - bq_0$, o resultado é válido para $i = 0$. Suponhamos, por hipótese de indução que o resultado é verdadeiro para i e para $i - 1$. Então

$$\begin{aligned} r_{i+1} &= r_{i-1} - r_i q_{i+1} \\ &= u_{i-1} a + v_{i-1} b - (u_i a + v_i b) q_{i+1} \\ &= (u_{i-1} - u_i q_{i+1}) a + (v_{i-1} - v_i q_{i+1}) b \\ &= u_{i+1} a + v_{i+1} b \end{aligned}$$

Portanto, para qualquer $0 \leq i \leq k$, $r_i = u_i a + v_i b$. Em particular, existem inteiros u e v, tais que $r_k = ua + vb$. $\square$

Exemplo. *Seja $a = 543$ e $b = 431$. A seguinte tabela esquematiza o algoritmo de Euclides para calcular $d = (a, b)$ e descobrir u e v tais que $au + bv = 1$.*

i	-2	-1	0	1	2	3	4	5	6
q_i			1	3	1	5	1	1	2
r_i	543	431	112	95	17	10	7	3	1
u_i	1	0	1	-3	4	-23	27	-50	127
v_i	0	1	-1	4	-5	29	-34	63	-160

Então $(a, b) = 1$ e $127a - 160b = 1$. Mais, para cada $-2 \leq i \leq k$ $r_i = au_i + bv_i$.

Teorema 3.2. *Suponhamos que $a > b$. Então*

tempo(determinar (a, b) usando o algoritmo de Euclides) $= O(\log^3 a)$.

Demonstração: O algoritmo de Euclides consiste em efectuar sucessivas divisões, onde os sucessivos restos formam uma sequência estritamente decrescente. Portanto, para estimar o número de operações bit, precisamos de saber quantas divisões é necessário efectuar. Primeiro, vamos provar que $r_{i+2} < \frac{1}{2} r_i$:

Se $r_{i+1} \leq \frac{1}{2} r_i$, então como $r_{i+2} < r_{i+1}$, obtemos $r_{i+2} < \frac{1}{2} r_i$.

Se $r_{i+1} > \frac{1}{2} r_i$, então a divisão seguinte, no algoritmo de Euclides, é

$$r_i = r_{i+1} + r_{i+2}.$$

Portanto, $r_{i+2} = r_i - r_{i+1} < \frac{1}{2} r_i$.

Acabámos de provar que em cada dois passos do algoritmo de Euclides o resto é pelo menos reduzido a metade, donde temos no máximo $2[\log_2 a]$ divisões. Como cada divisão envolve números menores ou iguais a a, o número de operações bit por divisão é $O(\log^2 a)$. Portanto, o algoritmo de Euclides demora

$$O(\log^3 a)$$

operações bit. $\square$

Definição. Sejam a e b inteiros tais que pelo menos um deles é não nulo. Se $(a, b) = 1$ então dizemos que a e b são *primos entre si.*

Teorema 3.3. *Se $(n, a) = 1$ e $n|ab$, então $n|b$.*

Demonstração: Pelo teorema 3.1, se $(n, a) = 1$ então existem inteiros u e v, tais que $nu + av = 1$, donde $nbu + abv = b$. Como $n|ab$, obtemos $n|b$. $\square$

Teorema 3.4. *Se $(a, n) = 1$ e $ab \equiv ac \mod n$, então $b \equiv c \mod n$. Em geral, se $(a, n) = d$ e $ab \equiv ac \mod n$ então*

$$b \equiv c \mod \frac{n}{d}.$$

Demonstração: Suponhamos que $(a, n) = d$ e $ab \equiv ac \mod n$. Então existe um inteiro k tal que $ab = ac + kn$. Sejam

$$a_1 = \frac{a}{d}, \quad n_1 = \frac{n}{d}.$$

Claramente, a_1 e n_1 são inteiros e $(a_1, n_1) = 1$. Dividindo ambos os membros de $ab = ac + kn$ por d, obtém-se $a_1(b - c) = kn_1$. Donde, $a_1 \mid kn_1$. Como $(a_1, n_1) = 1$, temos $a_1 \mid k$. Portanto, $k = a_1k_1$, para algum inteiro k_1. Assim, $b - c = k_1n_1$, ou seja $n_1 \mid (b - c)$. Portanto, $b \equiv c \mod \frac{n}{d}$. $\square$

Teorema 3.5. *Sejam a e b inteiros não nulos e $d = (a, b)$. Se $d \nmid c$ então a equação*

$$ax + by = c \tag{3.3}$$

não tem soluções inteiras. Se $d|c$, a equação tem uma infinidade de soluções inteiras. Se $x = x_0$, $y = y_0$ é uma solução de (3.3), então todas as soluções de (3.3) são dadas por

$$x = x_0 + t\frac{b}{d}$$
$$y = y_0 - t\frac{a}{d}$$

onde t é um inteiro.

Demonstração: Como $d|a$ e $d|b$, temos $d|(ax+by)$ para quaisquer inteiros x e y. Portanto, se $c = ax+by$, então $d|c$. Donde, se $d \nmid c$, (3.3) não tem soluções inteiras. Agora, se $d|c$, existe um inteiro e tal que $c = de$. Pelo teorema 3.1, existem inteiros u e v, tais que

$$au + bv = d.$$

Multiplicando por e, obtemos $a(ue) + b(ve) = de = c$. Portanto, a equação (3.3) tem pelo menos uma solução. Seja (x_0, y_0) uma solução de (3.3) e t um inteiro qualquer. Então

$$a\left(x_0 + t\frac{b}{d}\right) + b\left(y_0 - t\frac{a}{d}\right) = ax_0 + by_0 = c.$$

O que prova que a equação (3.3) tem uma infinidade de soluções.

Falta-nos ainda provar que qualquer solução de $ax+by = c$ é da forma descrita no teorema. Suponhamos que (x_1, y_1) é outra solução. Então

$$a(x_1 - x_0) + b(y_1 - y_0) = c - c = 0.$$

Donde

$$\frac{a}{d}(x_1 - x_0) = -\frac{b}{d}(y_1 - y_0), \tag{3.4}$$

o que implica que

$$\frac{b}{d} \mid \frac{a}{d}(x_1 - x_0).$$

Como $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$, temos $\frac{b}{d} \mid (x_1 - x_0)$. Portanto, existe um inteiro t, tal que

$$x_1 = x_0 + t\frac{b}{d}.$$

Substituindo em (3.4), obtemos

$$\frac{a}{d}t\frac{b}{d} = -\frac{b}{d}(y_1 - y_0),$$

donde

$$y_1 = y_0 - t\frac{a}{d}.$$

Portanto, qualquer solução de (3.3) é forma acima descrita. $\square$

Teorema 3.6. *A congruência*

$$ax \equiv b \mod n \tag{3.5}$$

tem soluções se e só se $d \mid b$, onde $d = (a, n)$. Se $d \mid b$ então a solução é única $\mod \frac{n}{d}$. *Se $(a, n) = 1$ então (3.5) tem uma solução que é única* $\mod n$.

Demonstração: Se x_0 é uma solução da equação (3.5) então existe um inteiro y_0 tal que

$$ax_0 = b + ny_0,$$

donde a equação

$$ax - ny = b \tag{3.6}$$

tem solução. Reciprocamente, se (x_0, y_0) é uma solução de (3.6) então

$$ax_0 \equiv ax_0 - ny_0 \equiv b \mod n$$

e, portanto, (3.5) tem solução. Acabámos de provar que (3.5) tem soluções se e só se (3.6) tem soluções e a partir de uma solução de (3.6) obtemos uma solução de (3.5). Pelo teorema 3.5, (3.6) tem soluções se e só se $d \mid b$. Portanto, (3.5) tem soluções se e só se $d \mid b$.

Suponhamos agora que (3.6) tem soluções e seja (x_0, y_0) uma solução. Pelo teorema 3.5 qualquer solução de (3.6) é da forma

$$x = x_0 + t\frac{n}{d}, \quad y = y_0 - t\frac{a}{d},$$

onde t é um inteiro. Portanto, qualquer solução de (3.5) é da forma

$$x = x_0 + t\frac{n}{d}$$

Como

$$x_0 + t\frac{n}{d} \equiv x_0 \mod \frac{n}{d},$$

então todas as soluções de (3.5) são congruentes com $x_0 \mod \frac{n}{d}$, e portanto, a solução de (3.5) é única $\mod \frac{n}{d}$.

A última parte do teorema resulta imediatamente das duas primeiras partes. □

Definição. Sejam a e n inteiros tais que $(a, n) = 1$. Ao único inteiro, que é solução da equação

$$ax \equiv 1 \mod n$$

chamamos *inverso* de $a \mod n$ e denota-mo-lo por $a^{-1} \mod n$.

Como o processo para escrever (a, b) como combinação linear de a e b é dado pelo algoritmo de Euclides, também este processo demora $O(\log^3 a)$ operações bit. Em particular obtemos:

Corolário 3.7. *Dado a, n inteiros, com $n > 1$ e $(a, n) = 1$. Então*

$$\textit{tempo(determinar } a^{-1}\textit{)} = O(\log^3 a).$$

Exemplo. *Como $(543, 431) = 1$ e $127 \cdot 543 - 160 \cdot 431 = 1$, então o inverso de $543 \mod 431$ é 127 e o inverso de $431 \mod 543$ é 383.*

3.7 Cifra Afim

Nesta subsecção, apresentamos outro caso especial da cifra de substituição, conhecido como cifra afim. Este tipo de criptosistema utiliza funções afins, i. e. funções da forma $f(x) = ax + b$. Mais uma vez utilizamos congruências para definir as regras para cifrar e para decifrar. Dado $m > 1$ inteiro, $a, b \in \mathbb{Z}_m$, queremos que a regra para cifrar $e_(x)$ (da cifra afim com a chave (a, b)) seja da forma

$$e(x) \equiv ax + b \mod m.$$

Note-se que, para podermos ter uma regra para decifrar é necessário que $e(x)$ seja injectiva. Pelo teorema 3.6, $e(x)$ é injectiva se e só se $(a, m) = 1$. Sabemos também que se $(a, m) = 1$ então a tem inverso $\mod m$.

Cifra (Afim)**.** *Seja m um inteiro positivo. Sejam $\mathcal{P} = \mathcal{C} = \mathbb{Z}_m$ e $\mathcal{K} = \{(a, b) \in \mathbb{Z}_m^2 \mid (a, m) = 1\}$. Sejam $x \in \mathcal{P}$ e $y \in \mathcal{C}$ então definimos*

$$e_{a,b}(x) \equiv ax + b \mod m$$

e

$$d_{a,b}(y) \equiv a^{-1}(y - b) \mod m$$

3.8 Função φ de Euler

Definição. Seja $n \geq 1$. O número de inteiros positivos menores ou iguais a n que são primos com n é denotado por $\varphi(n)$. Esta função de n é chamada *função φ de Euler*

Assim, o conjunto das chaves $\mathcal{K}$ tem $m\varphi(m)$ elementos. Recordamos agora os seguinte resultados sobre a função φ.

Teorema 3.8. *A função $\varphi(n)$ é multiplicativa.*

Demonstração: Sejam m e n inteiros positivos tais que $(m, n) = 1$. Vamos meter os primeiros mn inteiros numa tabela com m colunas e n linhas.

$$\begin{array}{cccc}
1 & 2 & \dots & \text{m} \\
\text{m+1} & \text{m+2} & \dots & \text{m+m} \\
\text{2m+1} & \text{2m+2} & \dots & \text{2m+m} \\
\vdots & \vdots & \vdots & \vdots \\
\text{(n-1)m+1} & \text{(n-1)m+2} & \dots & \text{(n-1)m+m}
\end{array}$$

Os números na coluna j são $m \cdot 0 + j$, $m \cdot 1 + j$, $m \cdot 2 + j, \dots, m(n-1) + j$. Temos, $(ma + j, m) = (j, m)$, para qualquer inteiro a. Portanto, ou qualquer elemento da coluna j é primo com m ou nenhum elemento da coluna j é primo com m. Assim, há exactamente $\varphi(m)$ colunas contendo inteiros primos com m e qualquer elemento destas $\varphi(m)$ colunas é primo com m.

Como $(m, n) = 1$, os n elementos de cada coluna j formam um sistema completo de resíduos $\mod n$. Portanto, por definição, cada coluna j contém exactamente $\varphi(n)$ elementos primos com n. Donde, em cada uma das $\varphi(m)$ colunas que têm os elementos que são primos com m, há exactamente $\varphi(n)$ elementos primos com n. Mais, estes são os únicos elementos que são ao mesmo tempo primos com m e primos com n. Isto é, há exactamente $\varphi(m)\varphi(n)$, elementos na tabela que são primos com m e, ao mesmo tempo, primos com n.

Mas um inteiro é primo com mn se e só se for primo simultaneamente com m e com n. Portanto,

$$\varphi(mn) = \varphi(m)\varphi(n)$$

e a função de Euler é multiplicativa. $\square$

Teorema 3.9. *Suponhamos que a factorização de n em primos é a seguinte*

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$$

Então

$$\varphi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_k}) = \prod_{i=1}^{k} (p_i^{a_i} - p_i^{a_i - 1})$$

Demonstração: Vamos começar por calcular $\varphi(p^a)$, para p primo e $a \geq 1$. Um inteiro é primo com p^a excepto se for divisível por p. Os números de 1 a p^a que são divisíveis por p, são $1 \cdot p$, $2 \cdot p$, $\ldots$, $p^{a-1}p$. Portanto,

$$\varphi(p^a) = p^a - p^{a-1} = p^a(1 - \frac{1}{p}).$$

Mas como a função $\varphi(n)$ é multiplicativa, temos

$$\begin{aligned}
\varphi(n) &= \varphi(p_1^{a_1})\varphi(p_2^{a_2}) \cdots \varphi(p_k^{a_k}) \\
&= p_1^{a_1}(1 - \frac{1}{p_1}) p_2^{a_2}(1 - \frac{1}{p_2}) \cdots p_k^{a_k}(1 - \frac{1}{p_k}) \\
&= p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_k}) \\
&= n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_k})
\end{aligned}$$

□

3.9 Criptoanálise da Cifra Afim

Suponhamos que é interceptada uma mensagem que se sabe ter sido cifrada usando um criptosistema afim, e que o alfabeto utilizado tem $N = 26$ letras. As duas letras mais frequentes na mensagem são "J"e "C". Sabe-se também que a mensagem está em inglês, e que nesta língua, as letras mais frequentes são o "E"e o "T"(ver figura 3.1). Deduzimos assim que, provavelmente, o

"E"foi cifrado em "J"e que o "T"foi cifrado em "C". Para determinar as chaves só temos que resolver o sistema de congruências

$$\begin{aligned} 10c + d &\equiv 5 \mod 26 \\ 3c + d &\equiv 20 \mod 26 \end{aligned}$$

Exemplo. *Vamos decifrar a seguinte mensagem.*

ICFMGTICJWARGIJGTRWNKJGFKWABGOKWFK
RWCBKAWJZMJGCCWKGCKJOKCKFKXJGFGNJM
GFMAAWFWLMOGFGCWTRWGKCMAAMKTGJMKFG
OKPMTVGSIWGBJWNWJMGSIWTRWSIWGFKXJG
FGWWJGGCKFGFKBKJRKTITOGAWOKCWNJMG

As letras mais frequentes são o **G** *e o* **W**, *portanto assumimos que* **a** *foi cifrado em* **G** *e* **e** *foi cifrado em* **W**.

Obtemos as congruências $6u + v \equiv 0 \mod 26$ *e* $22u + v \equiv 4 \mod 26$. *Logo* $u = 10$ *ou* $u = 23$, *mas* u *tem de ser primo com* 26, *donde* $u = 23$ *e* $v = 18$.

Portanto, $a = 17$ *e* $b = 6$.

Exercício. *Decifre a mensagem que se sabe ter sido cifrada usando uma cifra afim e que o texto plano está na língua portuguesa.*

HJHRF MRHOH XHMIZ XDFJF HQRUI TMHHZ XDTYI
TMHZH JTXRD HHQZY HJZJF DRFUH YJZUI ZHFQT
SYRDF ZJVZM HYRXI FHDFU IZDZQ FMBTZ ZXIHX
HMIZX QFOZJ XZMZA QZMRJ ZUIHO HXQFM TJFTJ
HRXOF XUFXX FXXZU IROFXQ HMHXZ HQMZD
RHMHH MIZOH JHIZJ HIRDH IZJFX OZTIR YRWHM
FMHDR FDRUR FZTJY FUVFQ ZMRFO FOZIM ZRUFR
UIZUX REF

3.10 Cifra de Vigenère

Nas cifras estudadas até agora, dada uma chave, cada letra é transformada numa só outra letra. Por esta razão, aqueles criptosistemas são denominados mono-alfabéticos. A cifra de Vigenère, que vamos apresentar nesta secção, é o primeiro exemplo de um criptosistema poli-alfabético.

Cifra (Vigenère)**.** *Sejam m e n inteiros positivos. Sejam $\mathcal{P} = \mathcal{C} = \mathcal{K} = (\mathbb{Z}_m)^n$. Dada uma chave $K = (k_1, \ldots, k_n)$ e $x \in \mathcal{P}$ e $y \in \mathcal{C}$, definimos*

$$e_K(x_1, \ldots, x_n) \equiv (x_1 + k_1, \ldots, x_n + k_n) \mod m$$

e

$$d_K(y_1, \ldots, y_n) \equiv (y_1 - k_1, \ldots, y_n - k_n) \mod m.$$

O número de chaves possíveis, dados m e n é m^n.

Exemplo. *Suponhamos que $m = 26$, $n = 8$ e a chave é* PORTUGAL. *Então $K = (15, 14, 17, 19, 20, 6, 0, 11)$. Queremos cifrar a frase*

este criptosistema nao e seguro

Primeiro codificamos o texto plano depois ciframos grupos de 8 *de cada vez e adicionamos a chave* mod 26*, da seguinte maneira*

4	18	19	4	2	17	8	15	19	14	18	8	18	19	4
15	14	17	19	20	6	0	11	15	14	17	19	20	6	0
19	6	10	23	22	23	8	3	6	2	9	1	12	25	4

12	0	13	0	14	4	18	4	6	20	17	14
11	15	14	17	19	20	6	0	11	15	14	17
23	15	1	17	7	24	24	4	17	9	5	5

A mensagem cifrada fica

TGKXWXIDGCJBMZEXPBRHYYERJFF

3.11 Criptoanálise da cifra de Vigenere

O primeiro passo para criptanalisar a cifra de Vigenere consiste em encontrar o comprimento da palavra chave, que denotamos por n. Vamos estudar duas técnicas que nos podem ajudar a encontrar n, nomeadamente o *teste de Kasiski* e o *índice de coincidência*.

O teste de Kasiski foi pela primeira vez descrito por Friedrich Kasiski em 1863. Este teste tem por base o facto de dois segmentos idênticos do texto plano serão transformados no mesmo texto cifrado sempre que a sua ocorrência no texto plano está com x posições de separação, com $x \equiv 0 \mod n$. Reciprocamente, se forem observados no texto cifrado dois segmentos idênticos com comprimento de pelo menos três letras, então há uma grande chance que eles correspondam a segmentos idênticos do texto plano.

O teste de Kasiski funciona do seguinte modo: Primeiro procuramos no texto cifrado pares de segmentos idênticos de comprimento maior ou igual a 3 e guardamos a distância entre o início de cada um dos dois segmentos. Se obtivermos as distâncias $d_1, d_2, \ldots$ então conjecturamos que n divide o maior divisor comum entre todas as distâncias.

Outro processo para estimar o valor de n, consiste em utilizar o índice de coincidência desenvolvido por Wolfe Friedman em 1920.

Definição. Seja $x = x_1x_2 \ldots x_m$ uma lista de m letras. O *índice de coincidência* de x, que denotamos por $I_c(x)$ é a probabilidade de que dois elementos de x sejam iguais. Denotemos as frequências de $A, B, C, \ldots, Z$ em x por $f_0, f_1, \ldots, f_{25}$. Como podemos escolher dois elementos de x de $\binom{m}{2}$ maneiras e, para cada $0 \leq i \leq 25$, há $\binom{f_i}{2}$ maneiras de escolher dois elementos e ambos serem i então,

$$I_c(x) = \frac{\sum_{i=0}^{25} f_i(f_i - 1)}{m(m-1)}.$$

Se x é parte de um texto em inglês ou é um texto cifrado através de uma cifra mono-alfabética, e p_i são as probabilidades indicadas na figura 3.1 será de esperar que

$$I_c(x) \approx \sum_{i=0}^{25} p_i^2 = 0.065.$$

A figura 3.3 apresenta os índices de coincidência de várias línguas.

Português	0.0738
Inglês	0.0661
Francês	0.0778
Italiano	0.0738
Alemão	0.0762
Japonês	0.0819
Russo	0.0529
Texto aleatório	0.0385

Figura 3.3: Índices de Coincidência esperados

Vejamos agora como utilizar o índice de coincidência para determinar o comprimento da palavra passe de uma cifra de Vigenere, n.

Suponhamos que $y = y_1 y_2 \ldots y_m$ foi obtido através de uma cifra de Vigenere de um texto plano em inglês. Para cada inteiro $r \geq 1$, escrevemos a mensagem cifrada y, por colunas numa matriz do tipo $r \times m/r$. Denotamos por $\mathbf{y_i}$ a linha i, desta matriz, com $1 \leq i \leq r$. Se $r = n$ então é de esperar que $I_c(\mathbf{y_i})$ seja aproximadamente 0.0661, para qualquer $1 \leq i \leq r$. Se $r \neq n$ então as listas $\mathbf{y_i}$ serão mais aleatórias, pois foram obtidas utilizando cifras de deslocamento com várias chaves. Como o índice de coincidência esperado de uma língua é muito diferente do índice de coincidência esperado de um texto aleatório, seremos capazes de descobrir o valor de n.

Após determinarmos o comprimento da palavra passe, cada $\mathbf{y_i}$ é obtido através de uma cifra de deslocamento de um texto plano na língua considerada e pode ser utilizada a análise de frequências para obter a palavra passe. Quando o texto plano é pequeno, a análise de frequências pode não ser suficiente para conjecturar com grande convicção o valor da chave. Neste caso, usamos o *índice de coincidência mútua* entre duas listas.

Definição. Sejam $x = x_1 x_2 \ldots x_m$ e $y = y_1 y_2 \ldots y_t$ listas com m e t letras, respectivamente. O *índice de coincidência mútua* de x e y, que denotamos por $MI_c(x, y)$ é a probabilidade de um elemento de x ser igual a um elemento de y. Se denotarmos as frequências de $A, B, \ldots, Z$ em x e y por $f_0, f_1, \ldots, f_{25}$ e $g_0, g_1, \ldots, g_{25}$, respectivamente, então

$$MI_c(x, y) = \frac{\sum_{i=0}^{25} f_i g_i}{mt}.$$

Já vimos que cada $\mathbf{y_i}$ é obtido através de uma cifra de deslocamento.

Seja $K = (k_1, \ldots, k_n)$ a palavra passe, então $\mathbf{y_i}$ obtém-se somando k_i a cada i-ésima letra do texto plano. Vamos primeiro estimar $MI_c(\mathbf{y_i}, \mathbf{y_j})$. Tirando uma letra de $\mathbf{y_i}$ e outra de $\mathbf{y_j}$, a probabilidade de serem ambas A é $p_{-k_i}p_{-k_j}$, a probabilidade de ambas serem B é $p_{1-k_i}p_{1-k_j}$, etc. (note que os índices são reduzidos $\mod 26$). Portanto,

$$MI_c(\mathbf{y_i}, \mathbf{y_j}) \approx \sum_{h=0}^{25} p_{h-k_i}p_{h-k_j} = \sum_{h=0}^{25} p_h p_{h+k_i-k_j}.$$

Esta estimativa depende apenas da diferença $k_i - k_j \mod 26$ à qual chamamos *deslocamento relativo* de $\mathbf{y_i}$ e $\mathbf{y_j}$. Mais, como

$$\sum_{h=0}^{25} p_h p_{h+l} = \sum_{h=0}^{25} p_{h-l} p_h,$$

um deslocamento relativo de u dá a mesma estimativa para MI_c que um deslocamento relativo de $26 - u$. Portanto precisamos apenas de calcular as estimativas para os deslocamentos relativos entre 0 e 13.

Deslocamento relativo	Valor esperado de MI_c
0	0.065
1	0.039
2	0.032
3	0.034
4	0.044
5	0.033
6	0.036
7	0.039
8	0.034
9	0.034
10	0.038
11	0.045
12	0.039
13	0.043

Verifica-se que um deslocamento relativo nulo dá um índice de coincidência mútua (MI_c) muito distinto do MI_c correspondente a qualquer outro deslocamento relativo. Podemos usar esta informação para tentar descobrir $u = k_i - k_j$. Primeiro fixamos $\mathbf{y_i}$ e vamos cifrar $\mathbf{y_j}$ usando cada uma das chaves g com $0 \leq g \leq 25$ e denotamos a mensagem cifrada obtida, por $\mathbf{y_j^g}$. Em seguida, calculamos os índices $MI_c(\mathbf{y_i}, \mathbf{y_j^g})$, para cada $0 \leq g \leq 25$,

$$MI_c(\mathbf{y_i}, \mathbf{y_i^g}) = \frac{\sum_{h=0}^{25} f_{h,i} f_{h-g,j}}{mt},$$

onde $f_{h,i}$ e $f_{h,j}$ são as frequências da letra correspondente a h em $\mathbf{y_i}$ e $\mathbf{y_j}$, respectivamente. Quando $g = u$ o índice MI_c deve ser próximo de 0.065, mas quando $g \neq u$ o índice deve ser relativamente menor. Para cada i e j devemos calcular 14 índices, um para cada chave.

Vamos ilustrar estes métodos com o seguinte exemplo:

Exemplo. *Sabemos que a seguinte mensagem foi cifrada utilizando um criptosistema de Vigenere.*

CHREEV OAHMAE RATBIA XXWTNX BEEOPH BSBQMQ
EQERBW RVXUOA KXAOSX XWEAHB WGJMMQ MNKGRF
VGXWTR ZXWIAK LXFPSK AUTEMN DCMGTS XMXBTU
IADNGM GPSREL XNJELX VRVPRT ULHDNQ WTWDTY
GBPHXT FALJHA SVBFXN GLLCHR ZBWELE KMSJIK
NBHWRJ GNMGJS GLXFEY PHAGNR BIEQJT AMRVLC
RREMND GLXRRI MGNSNR WCHRQH AEYEVT AQEBBI
PEEWEV KAKOEW ADREMX MTBHHC HRTKDN VRZCHR
CLQOHP WQAIIW XNRMGW OIIFKE E

Primeiro, vamos tentar descobrir n utilizando o teste de Kasiski. O trigrama CHR *aparece cinco vezes na mensagem cifrada, começando nas posições* $1, 166, 236, 276$ *e* 286. *As distâncias da primeira ocorrência às outras são* $165, 235, 275$ *e* 285 *e o máximo divisor comum entre estes valores é* 5. *Portanto, é de prever que o comprimento da palavra passe seja* 5.

Vejamos se com o cálculo dos índices de coincidência chegamos à mesma conclusão. Se $r = 1$, *o índice de coincidência é* 0.045. *Se* $r = 2$ *obtemos* $I_c(\mathbf{y_1}) = 0.046$ *e* $I_c(\mathbf{y_2}) = 0.041$. *Se* $r = 3$ *obtemos* $I_c(\mathbf{y_1}) = 0.043, I_c(\mathbf{y_2}) = 0.050$ *e* $I_c(\mathbf{y_3}) = 0.047$. *Para* $r = 4$, *obtemos os valores* $0.042, 0.039, 0.046$ *e* 0.040. *Finalmente, para* $r = 5$, *obtemos* $0.063, 0.068, 0.069, 0.061$ *e* 0.072, *o que também sugere que* $n = 5$.

Vamos agora tentar utilizar os índices de coincidência mútua para descobrir a palavra passe. Utilizando um programa no computador, calcula-se todos os 260 *valores de* $MI_c(\mathbf{y_i}, \mathbf{y_j^g})$, *com* $1 \leq i < j \leq 5$ *e* $0 \leq g \leq 25$, *e*

procura-se os valores que forem próximos de 0.065*. Dado um par* (i, j)*, se houver um único valor perto de* 0.065*, conjecturamos que esse é o valor do deslocamento relativo.*

Verifica-se haver grande evidência que o deslocamento relativo entre $\mathbf{y_1}$ *e* $\mathbf{y_2}$ *seja* 9*; o deslocamento relativo entre* $\mathbf{y_2}$ *e* $\mathbf{y_3}$ *seja* 13*; o deslocamento relativo entre* $\mathbf{y_2}$ *e* $\mathbf{y_5}$ *seja* 7*; o deslocamento relativo entre* $\mathbf{y_3}$ *e* $\mathbf{y_5}$ *seja* 20*; o deslocamento relativo entre* $\mathbf{y_4}$ *e* $\mathbf{y_5}$ *seja* 11*. Obtemos assim as seguintes equações nas cinco incógnitas* $k_1, \ldots, k_5$ *(todos os cálculos são efectuados* mod 26*):*

$$\begin{aligned}
k_1 - k_2 &= 9 \\
k_1 - k_5 &= 16 \\
k_2 - k_3 &= 13 \\
k_2 - k_5 &= 7 \\
k_3 - k_5 &= 20 \\
k_4 - k_5 &= 11.
\end{aligned}$$

Donde

$$\begin{aligned}
k_2 &= k_1 + 17 \\
k_3 &= k_1 + 4 \\
k_4 &= k_1 + 21 \\
k_5 &= k_1 + 10
\end{aligned}$$

Assim, a chave deve ser $(k_1, k_1 + 17, k_1 + 4, k_1 + 21, k_1 + 10)$*, para algum* $0 \leq k_1 \leq 25$*, ou seja, a chave é uma das sequências* AREVK *ou* BSFWL *ou* CTGXM.... *A única destas sequências que faz sentido é* $JANET$*. Note-se que a palavra passe não tem que fazer sentido. Nesse caso, podemos experimentar qualquer das possíveis chaves até que uma dê um texto com sentido, ou, se quisermos utilizar o computador, verificar qual delas é que corresponde a um texto plano que tenha uma análise de frequências de acordo com a língua que está a ser utilizada. Para a chave* JANET *Obtemos o texto plano*

> The almond tree was in tentative blossom. The days were longer, often ending with magnificent evenings of corrugated pink skies.

The hunting season was over, with hounds and guns put away for six months. The vineyards were busy again as the well-organized farmers treated their vines and the more lackadaisical neighbors hurried to do the pruning they should have done in November.

3.12 Cifra de Hill

Nesta secção descrevemos outro criptosistema polialfabético inventado em 1929 por Lester S. Hill.

Cifra (Hill)**.** *Sejam m e n inteiros positivos. Sejam $\mathcal{P} = \mathcal{C} = (\mathbb{Z}_m)^n$ e $\mathcal{K} = \{K \in \mathcal{M}_n(\mathbb{Z}_m) : K$ é invertível$\}$. Dada uma chave*

$$K = \begin{pmatrix} k_{1,1} & k_{1,2} & \dots & k_{1,n} \\ k_{2,1} & k_{2,2} & \dots & k_{2,n} \\ \vdots & \vdots & & \vdots \\ k_{n,1} & k_{n,2} & \dots & k_{n,n} \end{pmatrix}$$

e $x \in \mathcal{P}$ e $y \in \mathcal{C}$, definimos

$$e_K(x_1, x_2, \dots, x_n) \equiv (x_1\ x_2\ \dots\ x_n)K \mod m$$

e

$$d_K(y_1, y_2 \dots, y_n) \equiv (y_1\ y_2\ \dots\ y_n)K^{-1} \mod m.$$

Exemplo. *Sejam $m = 26$, $n = 2$ e*

$$K = \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}$$

Neste caso

$$K^{-1} = \begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix}$$

Para cifrar o texto plano hill*, dividimos primeiro nos dois grupos* hi *e* ll *e efectuamos os produtos*

$$\begin{pmatrix} 7 & 8 \end{pmatrix} \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix} = \begin{pmatrix} 23 & 8 \end{pmatrix}$$

e

$$\begin{pmatrix} 11 & 11 \end{pmatrix} \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix} = \begin{pmatrix} 24 & 9 \end{pmatrix}$$

A mensagem cifrada fica XIYJ*.*

3.13 Ataque à cifra de Hill

A cifra de Hill é mais difícil de quebrar quando só se conhece a mensagem cifrada, mas sucumbe muito facilmente quando se conhece um texto plano que deu origem a uma mensagem cifrada. Vamos assumir que o oponente conhece o valor de n (comprimento de cada parte do texto plano a ser cifrada individualmente) e conhece pelo menos n pares distintos de n-uplos $x_j = (x_{j,1}, x_{j,2}, \ldots, x_{j,n})$ e $y_j = (y_{j,1}, y_{j,2}, \ldots, y_{j,n})$, tais que $y_j = e_K(x_j)$, com $1 \leq j \leq n$. Sejam $X = [x_{i,j}]$ e $Y = [y_{i,j}]$, então $Y = XK$, onde K é a matriz da chave desconhecida. Se X for invertível, o oponente pode obter $K = X^{-1}Y$ e quebrar o sistema. Se X não for invertível será necessário utilizar outros n pares.

Exemplo. *Suponha que o texto plano* friday *é cifrado utilizando uma cifra de Hill com* $n = 2$*, obtendo-se* PQCFKU*. Então temos* $e_K(5, 17) = (15, 16)$*,* $e_K(8, 3) = (2, 5)$ *e* $e_K(0, 24) = (10, 20)$*. Utilizando os dois primeiros pares, obtemos a equação matricial*

$$\begin{pmatrix} 15 & 16 \\ 2 & 5 \end{pmatrix} = \begin{pmatrix} 5 & 17 \\ 8 & 3 \end{pmatrix} K.$$

Como

$$\begin{pmatrix} 5 & 17 \\ 8 & 3 \end{pmatrix}^{-1} = \begin{pmatrix} 9 & 1 \\ 2 & 15 \end{pmatrix}$$

a chave K *é*

$$K = \begin{pmatrix} 9 & 1 \\ 2 & 15 \end{pmatrix} \begin{pmatrix} 15 & 16 \\ 2 & 5 \end{pmatrix} = \begin{pmatrix} 7 & 19 \\ 8 & 3 \end{pmatrix}.$$

Podemos utilizar o terceiro par para confirmar este resultado.

Mas pode acontecer (e é provável que aconteça) que o oponente não conheça n. Neste caso, ele pode usar este processo utilizando $n = 2, 3, \ldots$ até que a chave seja descoberta. Se um valor de n é incorrecto, então a matriz K obtida utilizando este algoritmo não funcionará para outros pares texto plano-texto cifrado. Portanto, n pode ser facilmente determinado.

3.14 Cifra de Permutação

Até agora todas as cifras estudadas envolveram substituições das letras do texto plano por letras da mensagem cifrada. A ideia da cifra de permutação