PAULO J. ALMEIDA
DIEGO NAPP

CRIPTOGRAFIA E SEGURANÇA

ENGEBOOK®

PAULO J. ALMEIDA
DIEGO NAPP

CRIPTOGRAFIA E SEGURANÇA

ENGEBOOK®

Autores
Paulo J. Almeida
Diego Napp

Título
Criptografia e Segurança

Editora
Publindústria, Edições Técnicas
Praça da Corujeira n.º 38 · 4300-144 PORTO
www.publindustria.pt

Distribuidor
Engebook – Conteúdos de Engenharia e Gestão
Tel. 220 104 872 · Fax 220 104 871
E-mail: apoiocliente@engebook.com · www.engebook.com

Revisão
Diogo Resende
Publindústria, Produção de Comunicação, Lda.

Design de capa
Luciano Carvalho
Publindústria, Produção de Comunicação, Lda.

Impressão
Impresso em Espanha
janeiro, 2017

Depósito Legal
419277/16

A **cópia ilegal** viola os direitos dos autores.
Os prejudicados somos todos nós.

Este livro encontra-se em conformidade com o novo Acordo Ortográfico de 1990, respeitando as suas indicações genéricas e assumindo algumas opções específicas.
Para uma maior coerência ortográfica, e nos casos em que esta situação se verifique, converteram-se todos os textos transcritos à nova ortografia, independentemente de a edição original ser ou não anterior à adoção do novo Acordo Ortográfico.

CDU
003.2 Sistemas de escrita
004 Ciência e tecnologia informáticas

ISBN
978-989-723-210-7 (Papel)
978-989-723-211-4 (E-book)

Engebook – Catalogação da publicação
Família: Informática
Subfamília: Segurança

PAULO J. ALMEIDA
DIEGO NAPP

CRIPTOGRAFIA E SEGURANÇA

ENGEBOOK®

Agradecimentos:

Os autores desejam agradecer a todos os seus alunos da unidade curricular Criptografia e Segurança, do mestrado em Matemática e Aplicações da Universidade de Aveiro, para os quais as notas que deram origem a este livro foram elaboradas, pelos imensos contributos que foram sempre transmitindo aos autores, ao longo de mais de 10 anos, nomeadamente Alexandre, Alexandra, Lídia, Lara, Olga, Rui, André, João Ramos, Salomé, Alexandra Alves, Alice, João Carvalho, Pedro, Andrea, Diogo, Joana, Lorena, José Alberto, Macarena, Sofia e Ruben.

Um enorme agradecimento a Helena Leite, a primeira aluna a efetuar a dissertação de mestrado sob a orientação de Paulo Almeida, e que com grande entusiasmo e empenho abraçou o sistema RSA e seus ataques, criou programas em Maple para ilustrar este fascinante tema, tendo explorado de uma forma exaustiva a literatura disponível, e pelo seu enorme contributo na elaboração deste trabalho.

Gostaríamos de agradecer de uma forma especial a Bruno Custódio, pela sua excelente dissertação de mestrado sobre fatorização e pelos espetaculares trabalhos em Maple, ainda tão utilizados, pelos alunos que o sucederam. Agradecemos também o seu enorme contributo para este trabalho.

Um agradecimento muito sentido a Ilídio Moreira, que infelizmente já não se encontra entre nós, pelo seu enorme entusiasmo pela matemática, pela sua ótima dissertação sobre Criptografia com Códigos, que foi o ponto de partida para Paulo Almeida desenvolver investigação nestas áreas e que culminou na escrita deste trabalho, com Diego Napp

Gostaríamos também de agradecer a Cláudia Sebastião, que tendo estudado o método da descida infinita de Fermat, no seu mestrado, encontra-se agora a trabalhar connosco em criptografia com códigos, pelas imensas conversas e pelo seu grande interesse pela matemática, e que uma nova edição deste trabalho irá de certeza ter contributos seus.

Devemos um agradecimento com muito carinho a Raquel Pinto, pelas infinitas conversas, pela imensa simpatia, por ter contribuído para uma grande ligação profissional e de amizade entre os autores, pelos inúmeros trabalhos de investigação efetuados connosco, e por ser uma pessoa fabulosa.

Um enorme agradecimento aos nossos colegas e amigos Rita Simões, Paolo Vettori e Sofia Pinheiro, pelas estimulantes conversas, por tantas vezes nos ouvirem e aconselharem, por serem especiais para nós.

Finalmente agradecemos às nossas companheiras, Maria e Tatiana, pela sua enorme paciência e carinho durante estes meses de trabalho no livro.

Introdução:

Alice deseja enviar uma mensagem a Bob sem que Eva a perceba, no caso desta intercetar a mensagem. Com este objetivo, 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 ações. Se Eva interceta 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.

Neste livro iremos aprender vários sistemas criptográficos, alguns dos quais são correntemente usados nas diversas comunicações de mensagens (militares, espionagem, números de PIN, conversações telefónicas, transações bancárias, Internet, e-mail, etc.). Ao mesmo tempo, estudaremos métodos para quebrar certas cifras e a razão pela qual alguns dos sistemas criptográficos são considerados inquebráveis. Sendo os autores matemáticos, foi dada muito ênfase à parte matemática da Criptologia, em particular à Teoria dos Números. As secções 3.4, 3.5, 4.1 e 4.4 tratam de resultados clássicos da teoria dos números, necessários para uma melhor compreensão do texto posterior. As subsecções 3.2.2, 6.4.1 e 6.5.1 são bastante técnicas e podem ser omitidas, numa primeira leitura.

Este livro está dirigido a estudantes e investigadores que estejam a estudar matemática, informática ou ciências da computação a um nível universitário e também aos professionais na área da segurança da informação. Estudantes que conheçam ferramentas essenciais da Teoria dos Números e algumas noções de Álgebra também poderão aproveitar e aprender com este livro.

Conteúdo

Capítulo 1

Preliminares

Neste capítulo iremos introduzir vários conceitos que serão utilizados ao longo do texto, assim como uma breve descrição histórica da criptografia.

1.1 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;

Emissor - Quem envia a mensagem;

Recetor - 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 denotarmos o espaço entre palavras por □ e fizermos a transformação □ → 0, A→ 1, ..., Z→ 26 então a palavra OLA passa 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;

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

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 recetor. O emissor e o recetor 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 o recetor tem a chave secreta);

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

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 é uma óptima área para ser usada em criptologia.

1.2 História

A história da criptografia aparenta ter sido iniciada no antigo Egipto, cerca de 1900 a.C. pelo arquiteto Khnumhotep II, no 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, Índia 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

considerou análises estatísticas para quebrar cifras, processo ainda usado na atualidade.

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 atualmente se chama *cifra de Vigenère*, por ter sido falsamente 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 *Câmeras 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 câmeras 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 retângulo 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 efetuar 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, efetua-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 efetuado 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).

Figura 1.2: Enigma, Bundesachiv. 1943/44

Após a Primeira Guerra Mundial 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 militares dos alemães e o envio de mensagens enganosas para os alemães localizados em França, conseguindo assim facilitar a invasão por Dunquerque.

O Japão tinha a Máquina Púrpura, cujo sistema foi quebrado por uma equipa da US Army Signals Intelligence Service, liderada por William Frederick Friedman (criador da palavra criptoanálise). William Friedman e Frank Rowlett desenvolveram a máquina criptográfica SIGABA, mas esta máquina era maior, mais pesada, mais cara, mais dificil de operar e mais frágil que o Enigma, e, embora muitos navios americanos possuissem uma, não foi utilizada nos campos de batalha. Outros sistemas tiveram de ser utilizados, nomeadamente o código Navajo, proposto por Philip Johnston.

Nos anos 60, o Dr. Horst Feistel, liderando um projeto 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, adota 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 fatorizar 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 (National Institute of Standards and Technology), que substituiu o NBS, 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, 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.

que é uma equação linear com m incógnitas. Se $n \geq 2m$ então temos um sistema de equações com m equações e m incógnitas e, portanto, pode ser resolvido. A seguinte equação matricial descreve este sistema de equações

$$(z_{m+1}, z_{m+2}, \ldots, z_{2m}) = (c_0, c_1, \ldots, c_{m-1}) \begin{bmatrix} z_1 & z_2 & \cdots & z_m \\ z_2 & z_3 & \cdots & z_{m+1} \\ \vdots & \vdots & & \vdots \\ z_m & z_{m+1} & \cdots & z_{2m-1} \end{bmatrix}.$$

Pode ser mostrado que a matriz tem inversa se m for o comprimento da chave secreta[1]. Neste caso, obtemos

$$(c_0, c_1, \ldots, c_{m-1}) = (z_{m+1}, z_{m+2}, \ldots, z_{2m}) \begin{bmatrix} z_1 & z_2 & \cdots & z_m \\ z_2 & z_3 & \cdots & z_{m+1} \\ \vdots & \vdots & & \vdots \\ z_m & z_{m+1} & \cdots & z_{2m-1} \end{bmatrix}^{-1}.$$

Vejamos um exemplo:

Exemplo 3.11.4 *Suponhamos que Óscar obtém a mensagem cifrada*

$$101101011110010$$

correspondente ao texto plano

$$011001111111000.$$

Então o fluxo de chaves pode ser obtido somando bit a bit mod 2 *os valores anteriores. Portanto o fluxo de chaves será*

$$1101001000010 10.$$

Então

$$(0,1,0,0,0) = (c_1, c_2, c_3, c_4, c_5) \begin{bmatrix} 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix}$$

Donde, após calcularmos a inversa da matriz e efetuar os restantes cálculos, obtemos $(c_1, c_2, c_3, c_4, c_5) = (1, 0, 0, 1, 0)$. *Portanto, a recorrência para gerar o fluxo de chaves é*

$$z_{i+5} \equiv z_i + z_{i+3} \mod 2.$$

[1] Ver exercício 1.9, pag 42, em *Criptography: Theory and Practice* de Douglas Stinson

Autoavaliação desde capítulo (soluções na secção 10):

1. Decifre a mensagem "PCMZCEMQ"que foi cifrada com uma cifra de Vigenère e chave secreta "DIEGO". Use $A = 0,\ B = 1, \ldots, Z = 25$.

2. Encontre a chave secreta e as seis primeiras letras desta mensagem que foi cifrada com a cifra afim:
"*qrgdfwsrcdzogycsrecfxgyqgdbgpecpxowmzctecsrecffecqzer fwyzwaowmzwapgqegyfzgyawpxerlmbfzewrojeqcmyeowmpeexc bwfwlicfzeicfgqyfwmpxeryfcpxgfqwidbefebocpxlgpxcawp xerlmbnwjyclferacrxygpgpxmyfroazereeterowmacpf*"

   Pode usar MAPLE para calcular as frequências. Use $A = 0,\ B = 1, \ldots Z = 25$.

3. A seguinte mensagem for cifrada com a cifra de Vigenère com um alfabeto de 26 letras:
"*anxkskyhbouleiwmgklsfmtazqmtaafituszdiyghefhfkm tuqfhxvjqmlazmtppdxbxpebokasztyvjaukzgoixaqnevhm eehazqrlzuuegjweullemtahemtbjkmstiseeyvjmnrvxfhx pjpiljghekpweshfggmnzlfouldueolltamtsfhxtsfivzsd ebtharmhffagktqanaaruehfpwhuvqrybd*"

   - Encontre o comprimento da chave.
   - Encontre a chave.
   - Decifre a 6 primeiras letras do texto original.

4. Cifre e decifre a mensagem AVEIRO (26 letras) usando a cifra de Hill com chave
$$K = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

5. Resolva
$$\begin{cases} x \equiv \ \ 2 \bmod 7 \\ x \equiv \ \ 3 \bmod 5. \end{cases}$$
   A solução é única em $\mathbb{Z}$?

6. Mostre que se $(a, n) = 1$ e $n \mid ab$ então $n \mid b$.

7. Seja $d = (a, n)$. Quando existem soluções de
$$ax \equiv b \bmod n?$$
   Se existe mais do que uma solução, que forma têm?

Publindústria, Edições Técnicas
Porto, 2017

CRIPTOGRAFIA E SEGURANÇA

PAULO J. ALMEIDA
DIEGO NAPP

Sobre o Livro

Este livro aborda o estudo de sistemas criptográficos, com a apresentação dos conceitos fundamentais e numerosos exemplos. O livro recolhe a experiência dos autores, lecionando há mais de 10 anos no ensino superior na matemática e em particular na área de criptologia. Procura-se com este livro explicar a teoria e os métodos aplicados na criptografia moderna.

Sobre os autores

Paulo J. Almeida é Professor Auxiliar no Departamento de Matemática da Universidade de Aveiro, Portugal. Fez o doutoramento na University of Georgia, nos Estados Unidos da América em 2004, na área de teoria dos números e realizou pós-doutoramento em Oxford, Reino Unido. O Prof. Almeida leciona as unidades curriculares Criptografia e Segurança e Teoria dos Números e Aplicações há mais de dez anos e é autor de várias publicações em revistas nternacionais. Os seus interesses científicos atuais são nas áreas da teoria de números, álgebra, teoria dos códigos e criptografia.

Diego Napp é investigador no Departamento de Matemática da Universidade de Aveiro, Portugal. Fez o doutoramento na Universidade de Groningen, na Holanda no 2008 nas área de teoria de sistemas e álgebra comutativa. Realizou pós-doutoramentos em Portugal (Aveiro e Porto) e Espanha (Valladolid e Castellón). O Prof. Napp é autor de mais de 30 publicações em revistas internacionais e tem dado cursos e conferencias em mais de 20 países. Os seus interesses científicos são nas áreas da teoria de sistemas, álgebra, teoria dos códigos e criptografia. Leciona atualmente a unidade curricular Criptografia e Segurança na Universidade de Aveiro.

Também disponível em formato *e-book*

ISBN: 978-989-723-210-7

9 789897 232107

www.**engebook**.com

ENGEBOOK®