

# 通信原理

## (英文版)

◆ 樊昌信 编著 ◆ 孙天义 英文审校

### Principles of Communications



電子工業出版社  
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY

<http://www.phei.com.cn>

# 通信原理

## (英文版)

Principles of Communications

樊昌信 编著 孙天义 英文审校

電子工業出版社

Publishing House of Electronics Industry

北京·BEIJING

### **Brief Introduction to the contents**

On the basis of introducing the principles of analog communication, the book is focused on the principles of digital communication, and describes the communication system constitute, the specifications, the operation principles, the performance analysis, and the design methods. New communication systems and technologies developed recently are emphasized.

The book is suitable for electronic specialties of engineering school in Chinese general institutions of higher learning as the textbook or reference for the junior and senior students and graduate students, and can also be used as a reference book or a textbook in the advanced study classes for the engineering and technical personnel engaged in communication engineering.

未经许可,不得以任何方式复制或抄袭本书之部分或全部内容。

版权所有,侵权必究。

#### **图书在版编目(CIP)数据**

通信原理:英文/樊昌信编著. —北京:电子工业出版社,2010.7

ISBN 978-7-121-10959-1

I. ①通… II. ①樊… III. ①通信理论 - 高等学校 - 教材 - 英文 IV. ①TN911

中国版本图书馆 CIP 数据核字(2010)第 095573 号

策划编辑:韩同平

责任编辑:韩同平 特约编辑:李佩乾

印 刷:涿州市京南印刷厂

装 订:涿州市桃园装订有限公司

出版发行:电子工业出版社

北京市海淀区万寿路 173 信箱 邮编: 100036

开 本: 787 × 1092 1/16 印张: 28.5 字数: 720 千字

印 次: 2010 年 7 月第 1 次印刷

印 数: 3 500 册 定价: 55.00 元

凡所购买电子工业出版社的图书,如有缺损问题,请向购买书店调换。若书店售缺,请与本社发行部联系,联系及邮购电话:(010) 88254888。

质量投诉请发邮件至 [zlts@phei.com.cn](mailto:zlts@phei.com.cn), 盗版侵权举报请发邮件至 [dbqq@phei.com.cn](mailto:dbqq@phei.com.cn)。

服务热线:(010) 88258888。

# Preface

---

In recent years, communication theory and technology has witnessed rapid development. In China, the application of telecommunication service has penetrated into almost every household and every person. The huge modern communication networks have been one of the important infrastructures in China. Correspondingly, the amount of telecommunication enterprises and employees there has also been increasing remarkably. Under this situation, the education of the new specialized personnel in the telecommunication field and the reeducation of the personnel in service have become important tasks. In addition, bilingual teaching is a new requirement in Chinese institutions of higher learning, and its importance has been recognized by more and more people. However, there is lack of appropriate textbooks in English on communication theory for Chinese students. This textbook is intended to accommodate the demand.

The current communication networks in China have almost all been digitized. Signals transmitted in China's public communication networks are mainly digital ones; only the signals transmitted in the user's loop and those signals for special applications are still analog. Hence, the discussion of analog signal transmission techniques is limited to a minimum, and the greater part of this book is devoted to discussions of digital communication including transforming, encoding and transmission of digital signals, as well as the digitization of analog signals.

In the discussion on digital communication technology, some new communication technologies have been emphasized, for example, trellis code modulation (TCM), orthogonal frequency division modulation (OFDM), multiple access, spread spectrum, TURBO code, and so on. Attention has been directed to the explanations that are associated with the application examples of the currently rapidly developed networks, such as satellite communication and computer communication networks, and so on.

In order to best possibly meet the teaching demand in different universities and the demand of the readers who are in active service, this book is divided into two parts. The first part constitutes the basic contents, and is essential for beginners. The second part contains the optional contents, and each chapter in this part is relatively independent. Some chapters in the second part can be selected for learning depending on teaching requirements, some of which can be used as reference for communication engineering personnel. In addition, considering the demands of different teaching programs and different teaching periods, some contents that have complicated calculations or proofs are printed under shadow. Those parts can be skipped over, without affecting understanding of the content that follows. Questions and exercises are provided at the end of each chapter. The questions can be used for review of the contents of each chapter, and can aid the readers in making a brief summary of the contents of each chapter by themselves. The exercises allow the readers to deeply grasp the contents of each chapter, to combine the theory with the practice, and to improve their ability to solve practical

problems. There are also some references at the end of this book for the readers to find the origins of the relevant conclusions. There are no more references listed, because during the network information era, the readers can easily obtain their required information from the Internet.

There are 7 chapters in the first part. The first chapter is focused on the introduction of communication, especially the basic concepts of digital communication and channels, and helps the readers build up a preliminary understanding. The second chapter elaborates on the characteristics of signals and the influence of channels on the transmission of signals. The third chapter briefly dwells on the principles of analog modulation systems. The fourth chapter discusses the sampling, quantization, and encoding methods of analog signals in detail. The fifth chapter gives a basic introduction of every aspect of the design of baseband transmission systems. The sixth chapter discusses the basic digital modulation systems in detail. The seventh chapter discusses synchronization including carrier synchronization, bit synchronization, group synchronization, and network synchronization, which is absolutely necessary for digital communication systems.

The second part consists of 7 chapters in total. The eighth chapter discusses the ideal performance of the system from the viewpoint of the optimum reception of digital signals, and the comparison of the optimum reception with that of the practical systems. The ninth chapter describes multichannel multiplexing and multiple access; specifically introducing some relevant international recommendations for the standards and some practical systems. The tenth chapter discusses error correcting coding and error control technology; the principles of error correcting coding with fine performance are emphasized. The eleventh chapter thoroughly discusses advanced digital modulation technologies on the basis of Chapter 6. The twelfth chapter describes the information theory. The performances of communication systems are analyzed using the fundamental theory in order to search for the optimum source coding methods and the optimum performances of the communication systems. The thirteenth chapter introduces various communication networks including telephone networks, data communication networks, integrated services digital networks and vehicle communication networks. The fourteenth chapter briefly introduces the principles of cryptography. Each chapter in Part 2 is relatively independent. Part 2 can be optionally studied based on demand, and its understanding will not be affected by skipping over some chapters (There is certain connection only between the Viterbi decoding algorithm in Chapter 10 and the TCM in Chapter 11.)

For the junior and senior students of general higher education institutions, lectures may be between 36 to 90 hours (or 2 to 5 credits) according to different specialties and different universities. The course may be arranged within one or two semesters, and supplemented by experiments.

The prerequisites for studying this book are mainly: analog electronic circuits, high frequency electronic circuits, digital logic circuits, linear algebra, probability theory, as well as signals and systems. For the students who have studied the course "Signals and Systems," the second chapter of this book may be briefly introduced as a review or just skipped over.

Fan Changxin  
Xidian University  
Xi'an, China

## Acknowledgements

I wish to express my sincerely deep gratitude to Dr.Sun Tianyi ( Professor Emeritus and former President of Xian International Studies University, Honorary Director and former Vice President of Translators Association of China) for his critical reviews of my manuscript and for numerous suggestions and corrections that have helped me shape the book into its present form.

I am very grateful to my editor at the Publishing House of Electronics Industry ,Mr. Han tong-ping, for his strong suggestion and encouragement of publishing the book. I am also greatly indebted to Xidian University for its support of writing the book.

Finally,I offer special thanks for some grammar clarifications to my granddaughter, Maretta H. Fan whose first language is English. She has checked a part of the manuscript.

# Contents

---

## PART I

<b>Chapter 1</b>	<b>Introduction</b>	(1)
1. 1	Historical Review of Communication	(1)
1. 2	Message, Information, and Signal	(2)
1. 3	Digital Communication	(3)
1. 3. 1	Basic Concept	(3)
1. 3. 2	Advantages of Digital Communication	(4)
1. 3. 3	Digital Communication System Model	(5)
1. 3. 4	Specifications of Digital Communication System	(7)
1. 4	Channel	(10)
1. 4. 1	Wireless Channel	(10)
1. 4. 2	Wired Channel	(15)
1. 4. 3	Channel Models	(18)
1. 4. 4	Influence of Channel Characteristics on Signal Transmission	(20)
1. 5	Noise in Channel	(23)
1. 6	Brief Summary	(25)
	Questions	(25)
	Exercises	(25)
<b>Chapter 2</b>	<b>Signals</b>	(27)
2. 1	Classification of Signals	(27)
2. 2	Characteristics of Deterministic Signals	(28)
2. 2. 1	Characteristics in Frequency Domain	(28)
2. 2. 2	Characteristics in Time Domain	(35)
2. 3	Characteristics of Random Signals	(35)
2. 3. 1	Probability Distribution of Random Variable	(36)
2. 3. 2	Probability Density of Random Variable	(37)
2. 4	Examples of Frequently Used Random Variables	(38)
2. 5	Numerical Characteristics of Random Variable	(39)
2. 5. 1	Mathematical Expectation	(39)

2. 5. 2	Variance .....	(40)
2. 5. 3	Moment .....	(41)
2. 6	Random Process .....	(41)
2. 6. 1	Basic Concept of Random Process .....	(41)
2. 6. 2	Stationary Random Process .....	(42)
2. 6. 3	Ergodicity .....	(43)
2. 6. 4	Autocorrelation Function and Power Spectral Density of Stationary Random Process .....	(44)
2. 7	Gaussian Process .....	(49)
2. 8	Narrow Band Random Process .....	(53)
2. 8. 1	Basic Concept of Narrow Band Random Process .....	(53)
2. 8. 2	Characteristics of Narrow Band Random Process .....	(53)
2. 9	Sinusoidal Wave plus Narrow Band Gaussian Process .....	(55)
2. 10	Signal Transfer through Linear Systems .....	(57)
2. 10. 1	Basic Concept of Linear Systems .....	(57)
2. 10. 2	Deterministic Signal Transfer through Linear Systems .....	(57)
2. 10. 3	Random Signal Transfer through Linear Systems .....	(61)
2. 11	Brief Summary .....	(63)
	Questions .....	(65)
	Exercises .....	(66)
<b>Chapter 3</b>	<b>Analog Modulation System .....</b>	<b>(68)</b>
3. 1	Introduction .....	(68)
3. 2	Linear Modulation .....	(69)
3. 2. 1	Amplitude Modulation (AM) .....	(70)
3. 2. 2	Double-sideband Modulation (DSB) .....	(72)
3. 2. 3	Single-Sideband Modulation (SSB) .....	(72)
3. 2. 4	Vestigial Sideband Modulation (VSB) .....	(74)
3. 3	Nonlinear Modulation .....	(75)
3. 3. 1	Basic Principles .....	(75)
3. 3. 2	Frequency Spectrum and Bandwidth of Modulated Signal .....	(77)
3. 3. 3	Reception of Angular Modulated Signal .....	(79)
3. 4	Brief Summary .....	(80)
	Questions .....	(80)
	Exercises .....	(81)
<b>Chapter 4</b>	<b>Digitization of Analog Signal .....</b>	<b>(82)</b>
4. 1	Introduction .....	(82)
4. 2	Sampling of Analog Signal .....	(82)
4. 2. 1	Sampling of Low-Pass Analog Signal .....	(82)
4. 2. 2	Sampling of Band-Pass Analog Signal .....	(85)
4. 2. 3	Analog Pulse Modulation .....	(88)

4.3	Quantization of Sampled Signal .....	(88)
4.3.1	Principles of Quantization .....	(88)
4.3.2	Uniform Quantization .....	(89)
4.3.3	Nonuniform Quantization .....	(91)
4.4	Pulse Code Modulation .....	(97)
4.4.1	Basic Principles of Pulse Code Modulation .....	(97)
4.4.2	Natural Binary Code and Fold Binary Code .....	(98)
4.4.3	Quantization Noise in PCM System .....	(100)
4.5	Differential Pulse Code Modulation .....	(100)
4.5.1	Principles of Differential Pulse Code Modulation .....	(100)
4.5.2	Quantization Noise and Signal to Quantization Noise Ratio in DPCM System .....	(102)
4.6	Delta Modulation .....	(103)
4.6.1	Principles of Delta Modulation .....	(103)
4.6.2	Quantization Noise in Delta Modulation System .....	(104)
4.7	Brief Summary .....	(106)
	Questions .....	(107)
	Exercises .....	(107)

## **Chapter 5 Representation and Transmission of Baseband Digital Signal ..... (108)**

5.1	Introduction .....	(108)
5.2	Coding Method of Character .....	(108)
5.3	Waveform of Baseband Digital Signal .....	(109)
5.4	Symbol Code Types of Baseband Digital Signals for Transmission .....	(111)
5.5	Frequency Characteristic of Baseband Digital Signal .....	(113)
5.5.1	Calculation of Power Spectral Density of $v_c(t)$ .....	(115)
5.5.2	Calculation of Power Spectral Density of $u_c(t)$ .....	(115)
5.5.3	Calculation of Power Spectral Density of $s(t)$ .....	(116)
5.5.4	Examples of Power Spectral Density Calculation .....	(117)
5.6	Transmission and Intersymbol Interference of Baseband Digital Signal .....	(118)
5.6.1	Model of Baseband Digital Signal Transmission System .....	(118)
5.6.2	Intersymbol Interference and Nyquist Criterion .....	(119)
5.6.3	Partial Response System .....	(122)
5.7	Eye Pattern .....	(126)
5.8	Time-domain Equalizer .....	(128)
5.8.1	Introduction .....	(128)
5.8.2	Fundamental Principle of Transversal Filter .....	(128)
5.8.3	Realization of Transversal Filter .....	(132)
5.9	Brief Summary .....	(134)
	Questions .....	(135)
	Exercises .....	(135)

<b>Chapter 6 Elementary Digital Modulation System .....</b>	<b>(138)</b>
6. 1 Introduction .....	(138)
6. 2 Binary Amplitude Shift Keying (2ASK) .....	(140)
6. 2. 1 Basic Principle .....	(140)
6. 2. 2 Power Spectral Density .....	(140)
6. 2. 3 Symbol Error Probability .....	(142)
6. 3 Binary Frequency Shift Keying (2FSK) .....	(147)
6. 3. 1 Basic Principle .....	(147)
6. 3. 2 Power Spectral Density .....	(149)
6. 3. 3 Minimum Frequency Space .....	(150)
6. 3. 4 Symbol Error Probability .....	(151)
6. 4 Binary Phase Shift Keying (2PSK) .....	(155)
6. 4. 1 Basic Principle .....	(155)
6. 4. 2 Power Spectral Density .....	(157)
6. 4. 3 Symbol Error Probability .....	(158)
6. 5 Binary Differential Phase Shift Keying (2DPSK) .....	(159)
6. 5. 1 Basic Principle .....	(159)
6. 5. 2 Power Spectral Density .....	(161)
6. 5. 3 Symbol Error Probability .....	(161)
6. 6 Performance Comparison of Binary Digital Keying Transmission System .....	(164)
6. 7 <i>M</i> -ary Digital Keying .....	(165)
6. 7. 1 <i>M</i> -ary Amplitude Keying ( <i>M</i> -ASK) .....	(166)
6. 7. 2 <i>M</i> -ary Frequency Shift Keying ( <i>M</i> -FSK) .....	(167)
6. 7. 3 <i>M</i> -ary Phase Shift Keying ( <i>M</i> -PSK) .....	(171)
6. 7. 4 <i>M</i> -ary Differential Phase Shift Keying ( <i>M</i> -DPSK) .....	(174)
6. 7. 5 Amplitude/Phase Combination Keying (APK) .....	(178)
6. 7. 6 Examples of <i>M</i> -ary Digital Keying Practical Systems .....	(180)
6. 8 Brief Summary .....	(181)
Questions .....	(182)
Exercises .....	(183)
<b>Chapter 7 Synchronization .....</b>	<b>(184)</b>
7. 1 Introduction .....	(184)
7. 2 Carrier Synchronization Method .....	(185)
7. 2. 1 Pilot Insertion Method .....	(185)
7. 2. 2 Direct Extraction Method .....	(186)
7. 2. 3 Performance of Carrier Synchronization .....	(189)
7. 3 Bit Synchronization .....	(192)
7. 3. 1 External Synchronization .....	(192)
7. 3. 2 Self Synchronization .....	(192)

7.3.3	Influence of Bit Synchronization Error on Symbol Error Probability .....	(195)
7.4	Group Synchronization .....	(196)
7.4.1	Introduction .....	(196)
7.4.2	Concentrated Insertion Method .....	(198)
7.4.3	Dispersed Insertion Method .....	(200)
7.4.4	Performance of Group Synchronization .....	(202)
7.5	Network Synchronization .....	(203)
7.5.1	Introduction .....	(203)
7.5.2	Open-loop Method .....	(204)
7.5.3	Closed-Loop Method .....	(206)
7.6	Brief Summary .....	(208)
Questions	.....	(209)
Exercises	.....	(210)

## PART Ⅱ

Chapter 8	Optimum Receiving of Digital Signal .....	(212)
8.1	Statistical Characteristics of Digital Signal .....	(212)
8.2	Optimum Reception Criterion of Digital Signal .....	(214)
8.3	Optimum Receiver for Deterministic Digital Signal .....	(216)
8.4	Symbol Error Probability of Optimum Receiver for Deterministic Digital Signal .....	(218)
8.5	Optimum Receiving of Random Phase Digital Signal .....	(222)
8.6	Optimum Receiving of Fluctuation Digital Signal .....	(225)
8.7	Performance Comparison of Practical Receiver and Optimum Receiver .....	(226)
8.8	Matched Filtering Receiving Principle of Digital Signal .....	(227)
8.8.1	Matched Filtering Receiving of Digital Signal .....	(227)
8.8.2	Correlation Receiving of Digital Signal .....	(231)
8.9	Optimum Baseband Transmission System .....	(233)
8.10	Brief Summary .....	(236)
Questions	.....	(237)
Exercises	.....	(237)

Chapter 9	Multiplexing and Multiple Access .....	(239)
9.1	Introduction .....	(239)
9.2	Frequency Division Multiplexing (FDM) .....	(241)
9.3	Time Division Multiplexing (TDM) .....	(242)
9.3.1	Plesiochronous Digital Hierarchy (PDH) .....	(244)
9.3.2	Multiple Connection and Symbol Rate Justification .....	(246)
9.3.3	Synchronous Digital Hierarchy (SDH) .....	(249)
9.4	Code Division Multiplexing (CDM) .....	(251)
9.4.1	Basic Principles .....	(251)

9.4.2	Orthogonal Code .....	(254)
9.4.3	Pseudo-random Code .....	(256)
9.5	Multiple Access .....	(261)
9.5.1	Frequency Division Multiple Access (FDMA) .....	(262)
9.5.2	Time Division Multiple Access .....	(263)
9.5.3	Multiple Access Techniques for Local Area Networks .....	(270)
9.6	Brief Summary .....	(274)
	Questions .....	(274)
	Exercises .....	(276)

## Chapter 10 Channel Coding and Error Control ..... (278)

10.1	Introduction .....	(278)
10.2	Basic Principles of Error Control Coding .....	(281)
10.3	Performance of Error Correction System .....	(284)
10.4	Parity-Check Codes .....	(285)
10.5	Linear Block Codes .....	(287)
10.6	Cyclic Codes .....	(292)
10.6.1	Concept of Cyclic Codes .....	(292)
10.6.2	Operation of Cyclic Codes .....	(293)
10.6.3	Coding of Cyclic Codes .....	(296)
10.6.4	Decoding of Cyclic Codes .....	(297)
10.6.5	Truncated Cyclic Codes .....	(297)
10.6.6	BCH Codes .....	(298)
10.6.7	RS Codes .....	(300)
10.7	Convolution Codes .....	(300)
10.7.1	Coding of Convolution Codes .....	(301)
10.7.2	Decoding of Convolution Codes .....	(302)
10.8	Turbo Codes and LDPC Codes .....	(306)
10.9	Brief Summary .....	(309)
	Questions .....	(311)
	Exercises .....	(311)

## Chapter 11 Advanced Digital Bandpass Modulation and Demodulation ..... (314)

11.1	Introduction .....	(314)
11.2	Offset QPSK and $\pi/4$ QDPSK .....	(314)
11.2.1	Offset QPSK .....	(314)
11.2.2	$\pi/4$ QDPSK .....	(315)
11.3	Minimum Shift Keying and Gaussian Minimum Shift Keying .....	(316)
11.3.1	Basic Principles of MSK Signals .....	(316)
11.3.2	Phase Continuity of MSK Signals .....	(317)
11.3.3	Orthogonal Expression of MSK Signals .....	(319)

11.3.4	Generation and Demodulation of MSK Signals .....	(320)
11.3.5	Power Spectrum of MSK Signals .....	(322)
11.3.6	Symbol Error Probability of MSK Signals .....	(323)
11.3.7	Gaussian MSK .....	(323)
11.4	Orthogonal Frequency Division Multiplexing .....	(323)
11.4.1	Introduction .....	(323)
11.4.2	Basic Principles of OFDM .....	(324)
11.4.3	Implementation of OFDM .....	(327)
11.5	Trellis Coded Modulation .....	(329)
11.5.1	Basic Concept of Trellis Coded Modulation .....	(329)
11.5.2	Generation of TCM Signals .....	(330)
11.5.3	Demodulation of TCM Signal .....	(332)
11.6	Spread Spectrum Modulation .....	(333)
11.6.1	Introduction .....	(333)
11.6.2	Direct-Sequence Spread Spectrum .....	(334)
11.6.3	Frequency-Hopping SS .....	(336)
11.6.4	Synchronization of SS Code .....	(337)
11.6.5	Separation of Multipath .....	(338)
11.7	Brief Summary .....	(340)
Questions	.....	(340)
Exercise	.....	(341)
<b>Chapter 12</b>	<b>Information Theory</b> .....	(342)
12.1	Entropy of Discrete Source .....	(342)
12.2	Discrete Channel Model .....	(343)
12.3	Joint Entropy and Conditional Entropy .....	(344)
12.4	Noiseless Channel Capacity .....	(345)
12.5	Source Coding .....	(347)
12.5.1	Principles of Noiseless Channel Coding .....	(347)
12.5.2	Efficiency and Classification of Source Coding .....	(350)
12.5.3	Entropy of Extended Binary Source .....	(351)
12.5.4	Shannon-Fano Code .....	(351)
12.5.5	Huffman Code .....	(352)
12.6	Capacity of White Additive Gaussian Noise Channel .....	(353)
12.7	Brief Summary .....	(357)
Questions	.....	(357)
Exercises	.....	(358)
<b>Chapter 13</b>	<b>Communication Networks</b> .....	(360)
13.1	Types of Communication Networks .....	(360)
13.2	Telephone Networks .....	(362)

13. 2. 1	Structure of Telephone Networks .....	(362)
13. 2. 2	Switch in Telephone Networks .....	(363)
13. 2. 3	Signaling in Telephone Network .....	(363)
13. 2. 4	Performance of Telephone Network .....	(365)
13. 3	Data Communication Networks .....	(366)
13. 3. 1	Introduction .....	(366)
13. 3. 2	Switches in Data Communication Networks .....	(367)
13. 3. 3	Principles of Packet Switching .....	(368)
13. 3. 4	Open Systems Interconnection Reference Model .....	(370)
13. 3. 5	Architecture of Internet .....	(372)
13. 4	Integrated Services Digital Networks (ISDN) .....	(372)
13. 4. 1	Narrow-band Integrated Services Digital Networks (N-ISDN) .....	(372)
13. 4. 2	Broadband Integrated Services Digital Network (B-ISDN) .....	(374)
13. 5	Vehicle Communication Network .....	(378)
13. 5. 1	Introduction .....	(378)
13. 5. 2	Cell Partition and Frequency Programming of Cellular Networks .....	(378)
13. 5. 3	Constitution of Cellular Networks .....	(380)
13. 5. 4	System of Second Generation Cellular Networks .....	(380)
13. 5. 5	Third Generation Cellular Networks .....	(382)
13. 5. 6	Satellite Vehicle Communication Networks .....	(383)
13. 6	Brief Summary .....	(384)
Questions	.....	(386)
Exercises	.....	(387)
<b>Chapter 14</b>	<b>Communication Security .....</b>	<b>(388)</b>
14. 1	Introduction .....	(388)
14. 2	Single-key Cryptography Communication System .....	(389)
14. 3	Block and Stream Ciphers .....	(390)
14. 4	Information-Theoretic Approach for Cryptography .....	(391)
14. 4. 1	Perfect Security .....	(392)
14. 4. 2	Unicity Distance .....	(393)
14. 4. 3	Role of Data Compression in Cryptography .....	(394)
14. 4. 4	Diffusion and Confusion .....	(394)
14. 5	Data Encryption Standard .....	(396)
14. 6	Public Key Cryptography .....	(398)
14. 6. 1	Basic Principles .....	(398)
14. 6. 2	Diffie-Hellman Public Key Distribution .....	(399)
14. 7	RSA algorithm .....	(400)
14. 7. 1	RSA Public Key Cryptographic System .....	(400)
14. 7. 2	Application of RSA Algorithm in Digital Signatures .....	(401)
14. 8	Brief Summary .....	(402)

Questions .....	(402)
Exercises .....	(403)
Appendix A Parseval's Theorem .....	(404)
Appendix B Error function .....	(405)
Appendix C ASCII code .....	(407)
Appendix D CCITT No. 5 code .....	(408)
Appendix E China Standard 7 bit code .....	(409)
Appendix F Bessel functions .....	(409)
Appendix G Galois field $GF(2^m)$ .....	(410)
Appendix H Often-Used Identities and Constants .....	(411)
Abbreviations .....	(412)
Glossary .....	(415)
References .....	(420)
Index .....	(423)

# PART I

## Chapter 1

### Introduction

#### 1. 1 Historical Review of Communication

In centuries-old China, the origin of communication may at least be traced back to the Zhou dynasty. The old Chinese story about Emperor Zhou You Wang playing tricks on his dukes by ill-using beacon-fire (signal-fire) in the Zhou dynasty (781 ~ 771 B. C.) is well-known to all. This story is an evidence of the application of optical communication in ancient times. It is proved that the application of optical communication in China can be traced to as early as 800 B. C., which was the cutting edge technology of the world. Beacon-fire (Signal-fire) is a very primitive type of optical communication, and is also the simplest binary digital communication. It utilizes the existence or naught of optical signals to represent the enemy activities. Generally speaking, communication is the transfer of information. Now, there are two kinds of communication modes: transfer of information by manpower or mechanical method, e. g., the postal service-moving communication; or transfer of information by electricity (including current, radio, and optical wave), i.e. telecommunication. The discussion in this book is confined to the latter.

Modern telecommunication technology began in 1820 when A. M. Ampère invented telegraph communication. It was the beginning of the modern digital communication<sup>[1]</sup>. Hereafter, telegraph technology improved constantly. It developed rapidly and gained comprehensive application. Specifically, Samuel F. Morse put telegraph communication to practical application around 1838<sup>[1,2]</sup>. A.G. Bell invented telephone in 1876<sup>[3]</sup>. This is the beginning of analog communication. Telephone communication is a kind of real-time, interactive communication. It is more convenient than telegraph. After the 1960s, along with the emergence and development of semiconductor, computer, and laser technology, digital communication technology, which can transmit characters and computer data, entered advanced stage of development. Because advanced digital communication technology has many more advantages over analog communication in various aspects, some analog signals, such as speech and image, are preferably transmitted using digital communication technology. Hence, digital communication has been developing rapidly in the past 20 years or so. At the same time, optical fiber communication technology, an advanced optical communication technology, also progressed. Both have become the backbone of modern communication network.

The development of optical communication and digital communication mentioned above is one from the lowest to the highest stages.

## 1. 2 Message ,Information ,and Signal

The purpose of communication is to transfer information included in a message. For example, speech, letters, figures, and images are all messages. When people receive messages they are concerned about the effective content included in them, i.e. information. For example, when weather forecast is transferred, “fine” is expressed in the form of Chinese characters or a kind of symbols or figures. These representations are different types of messages, but they carry the same information. Messages is to be converted into electrical signals (generally called signals), then transmitted in a communication system. Therefore, signal is the carrier of message.

Information is the meaningful or effective content included in the message. As mentioned above, different types of messages may contain the same information. The amount of information transferred can be measured by “information content”, just as the amount of goods transported can be measured by the “volume of freight”. So, the first issue to be solved is how to measure information.

Messages are versatile. Hence, the method of measuring the information content included in the message should have no relation to the importance of the message. For example, “1 kg of gold stolen” and “1 kg of silver stolen” should contain the same information content, although gold is much more valuable than silver.

In all meaningful communication, the amount of the information content included in the same amount of message may be different to the receiver. For example, weather forecast “Rainfall will be 1 mm tomorrow” will bring the receiver no surprise; however, weather forecast “Rainfall will be 1 m tomorrow” will cause the receiver to jump out of his skin. It shows that messages may indeed contain different information contents. The more impossible the occurrence of the event expressed by the message, the more surprised the receiver, and the larger the information content. Therefore, we can use the uncertainty of the event, i.e. the probability of occurrence, to describe the magnitude of the information content. There is no need to transfer a message with certainty, e.g., “The sun will rise in the east tomorrow morning,” because the receiver has no interest in it. That is to say, the information content in a known message is zero.

We know from the probability theory that the uncertainty of an event can be described by the probability of its occurrence. When probability is used to describe information content, the smaller the probability of occurrence of the event expressed by the message, the larger the information content included. If the event expressed by the message is certain, its occurrence probability equals 1; then the information content of the message equals 0. The smaller the occurrence probability of the event, the larger the information content included. If the event is impossible, its occurrence probability equals 0, then the message will contain infinite information content. In addition, if the received message consists of several independent events, then the received total information content should be the sum of the information contents of these independent events.

According to the above description, the information content  $I$  contained in a message may be defined by the following method:

① Information content  $I$  contained in a message is a function of the occurrence probability  $P(x)$  of the message, i.e.

$$I = I[P(x)] \quad (1.2-1)$$

② The smaller the occurrence probability of a message, the larger the information content con-