

---

---

**A Diophantine Equations  
Based Cipher for  
Internet EDI Security in  
Macau**

---

---

**Fei Chun, Ma**

*Electrical & Electronics Engineering  
Faculty of Science & Technology  
University of Macau*

July 1997

# Contents

<b>1. INTRODUCTION</b>	<b>1</b>
1.1 MOTIVATION	1
1.2 ORGANIZATION OF THE THESIS	2
1.3 BIBLIOGRAPHY	3
<b>2. ELECTRONIC COMMERCE</b>	<b>4</b>
2.1 BRIEF HISTORY	4
2.2 EC IN MACAU	5
2.3 OVERVIEW OF EDI	5
2.4 EDI IN MACAU	7
2.5 INTERNET EDI	8
2.6 BIBLIOGRAPHY	9
<b>3. ARCHITECTURE OF INTERNET EDI</b>	<b>11</b>
3.1 OVERVIEW OF THE IMPLEMENTATION OF INTERNET EDI	11
3.2 EDI END USER INTERFACE	11
3.3 DATABASE MANAGEMENT SYSTEM	12
3.4 EDI TRANSLATOR	13
3.5 EDI STANDARDS	14
3.6 INTERNET EDI SECURITY SOFTWARE PACKAGE	18
3.7 INTERNET EDI COMMUNICATION PACKAGE AND NETWORK	18
3.8 BIBLIOGRAPHY	20
<b>4. SECURITY ISSUES FOR INTERNET EDI</b>	<b>22</b>
4.1 INTRODUCTION	22
4.2 MATHEMATICAL STRUCTURE OF SECRECY SYSTEMS	24
4.3 SIMPLE ENCRYPTION	25

<b>4.4 SYMMETRIC KEY CRYPTOGRAPHY</b>	<b>26</b>
<b>4.5 ASYMMETRIC KEY CRYPTOGRAPHY</b>	<b>28</b>
<b>4.6 DIGITAL SIGNATURE</b>	<b>29</b>
<b>4.7 MESSAGE DIGEST (MD)</b>	<b>30</b>
<b>4.8 DIGITAL CERTIFICATE &amp; CERTIFICATION AUTHORITY (CA)</b>	<b>32</b>
<b>4.9 BIBLIOGRAPHY</b>	<b>34</b>
<b><u>5. INTERNET TRANSFER PROTOCOLS FOR EDI</u></b>	<b><u>36</u></b>
<b>5.1 INTRODUCTION</b>	<b>36</b>
<b>5.2 SMTP (SIMPLE MAIL TRANSFER PROTOCOL)</b>	<b>37</b>
<b>5.3 FTP (FILE TRANSFER PROTOCOL)</b>	<b>39</b>
<b>5.4 HTTP (HYPER TEXT TRANSFER PROTOCOL)</b>	<b>42</b>
<b>5.5 BIBLIOGRAPHY</b>	<b>45</b>
<b><u>6. THE PROTOTYPE OF INTERNET EDI IN MACAU</u></b>	<b><u>47</u></b>
<b>6.1 INTRODUCTION</b>	<b>47</b>
<b>6.2 INTERNET EDI PROTOTYPE</b>	<b>48</b>
<b>6.3 THE DIOPHANTINE EQUATIONS BASED ASYMMETRIC KEY CIPHER</b>	<b>52</b>
<b>6.4 THE PROPOSED ASYMMETRIC KEY CIPHER AND THE PGP CIPHER COMPARISON</b>	<b>55</b>
<b>6.5 THE PRELIMINARY ANALYSIS OF THE EDI INTERCHANGE UNDER THE TCP/IP IN MACAU</b>	<b>57</b>
<b>6.6 BIBLIOGRAPHY</b>	<b>60</b>
<b><u>7. CONCLUSION</u></b>	<b><u>62</u></b>
<b>7.1 CONCLUDING REMARKS</b>	<b>62</b>
<b>7.2 OUTLINE OF FUTURE WORKS</b>	<b>66</b>
<b><u>APPENDIX A: AN EXAMPLE OF AN EDIFACT STANDARD FLAT FILE</u></b>	<b><u>67</u></b>
<b><u>APPENDIX B: SOURCE CODE OF DIOPHANTINE EQUATIONS BASED CIPHER</u></b>	<b><u>70</u></b>

<b>APPENDIX C: 100 GENERATED DES SESSION KEYS</b>	<b>73</b>
<b>APPENDIX D: PUBLIC AND PRIVATE KEYS FROM THE CIPHER</b>	<b>75</b>
<b>APPENDIX E: THE USED PGP PUBLIC KEY IN THIS THESIS</b>	<b>79</b>
<b>APPENDIX F: ENCRYPTION TIMING FOR THE CIPHERS</b>	<b>80</b>
<b>APPENDIX G: THE EDI E-MAIL FOR THE EXPERIMENTS</b>	<b>86</b>
<b>APPENDIX H: TRANSMISSION TIME FOR THE INTERNET IN MACAU</b>	<b>87</b>