

# Índice

<b>Prólogo .....</b>	<b>11</b>
<b>Capítulo I</b>	
<b>Introducción .....</b>	<b>13</b>
1.1 Desde la criptografía simétrica a la criptografía cuántica .....	13
1.2 El problema de la distribución de claves. Criptografía pública y PKI .....	15
<b>Capítulo II</b>	
<b>Sistemas de cifra clásica y su evolución a criptosistemas simétricos modernos .....</b>	<b>19</b>
<b>2.1 Introducción .....</b>	<b>19</b>
<b>2.2 Alfabetos y características del lenguaje .....</b>	<b>21</b>
2.2.1 Alfabetos de cifrado .....	21
2.2.2 Estadísticas del lenguaje .....	23
<b>2.3 Clasificación de los criptosistemas clásicos .....</b>	<b>26</b>
<b>2.4 Cifradores por sustitución .....</b>	<b>29</b>
2.4.1 Cifradores por sustitución monográfica monoalfabeto .....	29
2.4.2 Cifradores por homófonos .....	44
2.4.3 Cifradores por sustitución monográfica polialfabeto .....	51
2.4.4 Cifradores por sustitución poligráfica monoalfabeto .....	77
<b>2.5 Cifradores por transposición .....</b>	<b>102</b>
2.5.1 Transposición por grupos .....	104
2.5.2 Transposición por series .....	104
2.5.3 Transposición por columnas .....	105
2.5.4 Transposición por filas .....	110
2.5.5 Criptoanálisis de los cifrados por transposición .....	111

<b>2.6 De la cifra clásica a los cifradores modernos.....</b>	<b>114</b>
---	------------

## Capítulo III

<b>Criptografía de clave pública: El algoritmo RSA.....</b>	<b>121</b>
<b>3.1 Intercambio de clave de Diffie y Hellman.....</b>	<b>122</b>
<b>3.2 Principios del algoritmo RSA.....</b>	<b>124</b>
<b>3.3 Generación de claves para el algoritmo RSA.....</b>	<b>125</b>
3.3.1 Diseño y elección de claves RSA: valores de $p$ , $q$ y $e$ .....	127
3.3.2 Clave privadas y públicas parejas.....	131
<b>3.4 Cifrado y descifrado de información y mensajes.....</b>	<b>136</b>
3.4.1 Mensajes no cifrables .....	138
<b>3.5 Firma digital mediante el algoritmo RSA.....</b>	<b>143</b>
<b>3.6 RSA y el teorema chino del resto .....</b>	<b>145</b>
3.6.1 Cómo aplicar el TRC para ganar en eficiencia en aritmética modular .....	145
3.6.2 Aplicación del TRC en el descifrado de RSA.....	149
3.6.3 Precauciones en el uso del TRC en RSA.....	151
<b>3.7 Software OpenSSL. Practicando .....</b>	<b>152</b>
3.7.1 Generación de claves RSA con OpenSSL .....	152
3.7.2 Parámetros de OpenSSL para su uso en el TRC.....	158
<b>3.8 Ejercicios y prácticas .....</b>	<b>159</b>

## Capítulo IV

<b>La seguridad de la criptografía de clave pública y el algoritmo RSA.</b>	<b>171</b>
<b>4.1 Ataques criptoanalíticos al algoritmo RSA.....</b>	<b>171</b>
4.1.1 El problema de la factorización entera .....	172
4.1.2 Ataque por cifrado cíclico.....	178
4.1.3 Ataque por paradoja del cumpleaños.....	182
4.1.4 Recuperando textos en claro con exponente $e$ pequeño .....	188
<b>4.2 Seguridad de la criptografía pública en el mundo real.....</b>	<b>188</b>
4.2.1 Problemas derivados de fallos de implementación.....	188
4.2.2 Autoridades de certificación y PKI. Falsificando certificados digitales .....	189
4.2.3 Seguridad del protocolo SSL. Engañando al usuario .....	193

4.2.4 Mitigaciones y recomendaciones para el uso de HTTPS .....	196
<b>4.3 Ejercicios y prácticas .....</b>	<b>197</b>

## Capítulo V

### **Nuevos ataques en el marco de la criptografía pública.....209**

<b>5.1 La criptografía no se ataca, se esquivo. Escucha y almacena.....</b>	<b>210</b>
5.1.1 Proyecto Bullrun y Edgehill. Debilitando la criptografía.....	211
5.1.2 Almacena, que algo queda. Algoritmo GCD y big data .....	211
5.1.3 Ataques de canal lateral (side-channel). Tendencias.....	213
<b>5.2 Seguridad en TLS/SSL y en algoritmos de clave pública. Ataques modernos 214</b>	
5.2.1 CRIME y BREACH .....	214
5.2.2 Heartbleed.....	215
5.2.3 New Bleichenbacher side Channels and attacks.....	215
5.2.4 POODLE. Padding Oracle On Downgraded Legacy Encryption.....	216
5.2.5 SMACK y FREAK. State Machine Attacks on TLS .....	218
5.2.6 Logjam.....	218
5.2.7 SLOTH. Security Losses from Obsolete and Truncated Transcript Hashes.....	219
5.2.8 DROWN. Decrypting RSA with Obsolete and Weakened eNcryption .....	220
5.2.9 SWEET32. Birthday attacks on 64-bits block ciphers .....	220
5.2.10 ROCA – The Return of Coppersmith’s attack .....	221
5.2.11 The ROBOT. Return Of Bleichenbacher’s Oracle Threat .....	221

## Apéndice A

### **Fundamentos de Matemáticas Discretas.....223**

<b>1. Operaciones de congruencia en <math>Z_n</math> y conjunto de restos .....</b>	<b>223</b>
<b>2. Conjunto completo de restos CCR .....</b>	<b>224</b>
<b>3. El conjunto reducido de restos.....</b>	<b>224</b>
<b>4. La Función de Euler <math>\phi(n)</math> .....</b>	<b>224</b>
<b>5. Inversos en un cuerpo.....</b>	<b>225</b>
<b>6. El Teorema de Euler .....</b>	<b>226</b>
<b>7. Pequeño teorema de Fermat .....</b>	<b>227</b>
<b>8. Algoritmo Extendido de Euclides (AEE) .....</b>	<b>227</b>
<b>9. Exponenciación rápida .....</b>	<b>229</b>

## **Apéndice B**

<b>Teoría de la información.....</b>	<b>231</b>
1. ¿Qué es la teoría de la información?.....	231
2. Entropía de los mensajes, ratio y redundancia del lenguaje.....	234
3. La distancia de unicidad.....	238

## **Apéndice C**

<b>Software educativo.....</b>	<b>241</b>
<b>Índice de imágenes .....</b>	<b>245</b>
<b>Referencias y bibliografía recomendada.....</b>	<b>249</b>
<b>Índice alfabético .....</b>	<b>253</b>