

<b>Introduzione</b>	<b>6</b>
<b>1 Crittosistemi Classici</b>	<b>8</b>
1.1 Cifrari a blocchi . . . . .	8
1.2 Cifrario mediante sostituzione . . . . .	9
1.3 Cifrario Affine . . . . .	11
1.4 Cifrario mediante permutazione . . . . .	12
1.5 Cifrario di Vigenère . . . . .	13
1.6 Cifrario di Hill . . . . .	15
1.7 Cifrario mediante trasposizione . . . . .	16
1.8 Cifrari a flusso . . . . .	17
1.9 La macchina Enigma . . . . .	20
<b>2 Crittoanalisi</b>	<b>24</b>
2.1 Principio di Kerckhoffs . . . . .	24
2.2 Crittoanalisi del cifrario mediante sostituzione . . . . .	26
2.3 Crittoanalisi del cifrario affine e cifrario mediante permutazione . . . . .	27
2.4 Crittoanalisi del cifrario di Vigenère . . . . .	29
2.5 Crittoanalisi del cifrario di Hill . . . . .	33
<b>3 Segretezza Perfetta</b>	<b>34</b>
3.1 Criteri di Sicurezza . . . . .	34
3.2 Segretezza Perfetta . . . . .	35
3.3 Teorema di Shannon . . . . .	38
3.4 Cifrari Prodotto . . . . .	41
<b>4 Advanced Encryption Standard</b>	<b>43</b>
4.1 Cifrari Iterati . . . . .	43
4.2 Substitution-Permutation Network . . . . .	44
4.3 Advanced Encryption Standard . . . . .	48
4.3.1 Conversione Binario-Esadecimale-Elemento di $GF(2^8)$ . . . . .	49
4.4 Struttura . . . . .	51
4.4.1 SubBytes . . . . .	52
4.4.2 ShiftRows . . . . .	56
4.4.3 MixColumn . . . . .	57
4.4.4 AddRoundKey . . . . .	59
4.4.5 KeyExpansion . . . . .	59
4.5 Esempio di cifratura . . . . .	63

<b>5</b>	<b>Funzioni Hash Crittografiche</b>	<b>65</b>
5.1	Funzioni Hash . . . . .	65
5.2	MAC . . . . .	65
5.3	Sicurezza delle Funzioni Hash . . . . .	66
5.4	Il Modello dell'Oracolo Casuale . . . . .	67
5.5	Algoritmi nel Modello dell'Oracolo Casuale . . . . .	69
5.6	Confronto tra i criteri di sicurezza . . . . .	73
5.7	Funzioni Hash Iterate . . . . .	75
5.8	La costruzione di Merkle-Damgård . . . . .	76
5.9	SHA-1 . . . . .	81
5.10	Message Authentication Code (MAC) . . . . .	84
5.11	Nested MAC . . . . .	85
5.11.1	HMAC . . . . .	87
5.11.2	CBC – MAC . . . . .	87
5.12	MAC incondizionatamente sicuri . . . . .	89
5.12.1	Famiglie hash fortemente universali . . . . .	91
5.12.2	Ottimalità delle Probabilità di Inganno . . . . .	93
<b>6</b>	<b>Complessità computazionale di un algoritmo</b>	<b>96</b>
6.1	Rappresentazione di un intero in base $b$ . . . . .	96
6.2	Complessità temporale di un algoritmo . . . . .	97
6.3	Bit Operazioni . . . . .	98
6.3.1	Somma di due numeri di lunghezza binaria $k$ . . . . .	98
6.3.2	Prodotto di due numeri $n$ e $m$ di lunghezza binaria $k$ e $\ell$ , rispettivamente, con $k \geq \ell$ . . . . .	99
6.3.3	Algoritmo Euclideo . . . . .	102
6.3.4	Complessità delle operazioni in $\mathbb{Z}_n$ . . . . .	106
<b>7</b>	<b>Il Crittosistema RSA</b>	<b>108</b>
7.1	Elementi di Teoria dei Numeri . . . . .	108
7.2	Il Crittosistema RSA . . . . .	110
7.2.1	Implementare l'RSA . . . . .	112
<b>8</b>	<b>Test di Primalità</b>	<b>114</b>
8.1	Pseudoprimi . . . . .	124
8.1.1	Pseudoprimi di Eulero . . . . .	125
8.1.2	Pseudoprimi Forti . . . . .	126
8.2	Test di Primalità . . . . .	134
<b>9</b>	<b>Metodi di Attacco al Crittosistema RSA</b>	<b>139</b>
9.1	Radici quadrate modulo un intero . . . . .	139
9.2	Metodi di attacco al crittosistema RSA . . . . .	140
9.3	Algoritmo di Dixon per i quadrati casuali . . . . .	145
9.4	Altri metodi di attacco . . . . .	146
9.4.1	Calcolo di $\varphi(n)$ . . . . .	146
9.4.2	L'esponente di decifratura . . . . .	147

9.4.3	Attacco di Wiener . . . . .	149
<b>10</b>	<b>Problema del Logaritmo Discreto</b>	<b>155</b>
10.1	L'algoritmo di Shanks . . . . .	157
10.2	L'algoritmo Rho di Pollard . . . . .	159
10.3	L'algoritmo di Pohlig-Hellmann . . . . .	162
10.4	Il Metodo del Calcolo dell'Indice . . . . .	165
<b>11</b>	<b>Curve Ellittiche</b>	<b>168</b>
11.1	Curve Algebriche . . . . .	168
11.2	Legge di gruppo . . . . .	179
11.3	Numero di punti di una curva ellittica . . . . .	185
<b>12</b>	<b>Crittosistemi basati su curve ellittiche</b>	<b>187</b>
12.1	Costruzione di una curva ellittica . . . . .	187
12.2	Conversione delle unità di messaggio in chiaro in punti di una curva ellittica . . . . .	188
12.3	Logaritmo discreto su una curva ellittica . . . . .	190
12.4	Fattorizzare attraverso l'uso delle curve ellittiche . . . . .	193
12.4.1	Rappresentazione NAF . . . . .	193
12.4.2	Algoritmo di Lenstra . . . . .	196
<b>13</b>	<b>Firma Digitale</b>	<b>203</b>
13.1	Sistemi di Firma . . . . .	203
13.2	Combinare la firma digitale e la crittografia a chiave pubblica . .	205
13.3	Requisiti di sicurezza per i sistemi di firma . . . . .	206
13.4	Sistemi di firma e funzioni Hash . . . . .	207
13.5	Sistema di Firma di ElGamal . . . . .	208
13.6	Sicurezza del Sistema di Firma di ElGamal . . . . .	210
13.7	Varianti del Sistema di firma ElGamal . . . . .	212
13.7.1	Il Sistema di Firma di Schnorr . . . . .	212
13.7.2	L'Algoritmo di Firma Digitale . . . . .	215
13.7.3	L'Algoritmo di Firma Digitale basato sulle curve ellittiche (ECDSA) . . . . .	216
13.8	Il Sistema di Firma di Lamport . . . . .	218
13.9	Firme non ripudiabili . . . . .	222
13.10	Firme fail-stop . . . . .	229
	<b>Bibliografia</b>	<b>237</b>