

Indice

1	Introduzione	5
1.1	La collana “I quaderni della Settimana Matematica”	5
1.2	Crittografia	9
1.3	I percorsi possibili	11
2	Contenuti	15
2.1	La steganografia	17
2.1.1	Nascondere un messaggio	17
2.1.2	La steganografia antica	17
2.1.3	La steganografia moderna	17
2.2	I cifrari storici	19
2.2.1	La scitola	20
2.2.2	Il cifrario di Cesare	20
2.2.3	Il disco cifrante di Alberti	24
2.2.4	Il cifrario di Vigenère	26
2.2.5	Il codice ADFGVX	34
2.3	La crittografia incontra la matematica	37
2.3.1	La macchina Enigma	37
2.3.2	La crittografia a chiave asimmetrica	41
2.3.3	RSA	51
3	Gli strumenti matematici della crittografia	57
3.1	La spiegazione matematica di RSA	57
3.1.1	Acquisto e vendita su Internet	57
3.1.2	L’algoritmo di Euclide e il calcolo del M.C.D	59

3.1.3	L'identità di Bézout	67
3.1.4	Fare le operazioni “con i resti”: l'aritmetica modulare	71
3.1.5	Il Piccolo Teorema di Fermat	74
3.1.6	Torniamo a RSA!	76
3.2	Come viene effettivamente usato RSA?	81
3.3	Quanto è sicuro RSA?	83
4	Bibliografia	85