

## *Name index*

- Adelman, L. 171, 234  
 Andrews, G. E. 232
- Barker, W. G. 233  
 Beauchemin, P. 234  
 Beker, H. 233  
 Bell, E. T. 234  
 Berlekamp, E. R. 230  
 Brassard, G. 234  
 Brooke, R. 78
- Caesar, Julius *passim*  
 Chadwick, J. 230  
 Champollion, J. F. 230  
 Churchhouse, R. F. 232,  
 233  
 Clark, R. W. 231  
 Crepeau, C. 234
- Davies, D. W. 233, 234  
 Deavours, C. A. 232  
 Denham, H. C. 231  
 Dickens, C. 33  
 Diffie, W. 166, 233  
 Doyle, A. C. ix
- Ellis, J. 234  
 Estermann, T. 233  
 Eratosthenes 173  
 Euclid 192–3  
 Euler, L. 173, 175, 205, 211
- Feller, W. 232  
 Fermat, P. 173, 175, 234  
 Fibonacci *passim*  
 Fitzgerald, E. 218  
 Flannery, B. P. 232  
 Francis, W. N. 230  
 Friedman, W. F. 231
- Galbraith, S. 234  
 Galois, E. 216–7  
 ‘GARBO’ 9, 52, 88–92, 230, 232  
 Garfinkel, S. L. 234  
 Garlinski, J. 232  
 Gauss, C. F. 209, 233  
 Golomb, S. W. 232  
 Good, I. J. 31, 35, 132, 231  
 Goutier, C. 234
- Hadamard, J. 233  
 Hammersley, J. W. 232  
 Hamming, R. W. 8  
 Handscomb, D. C. 232  
 Hardy, G. H. 232, 233  
 Hellman, M. E. 166, 233  
 Hill, R. 230  
 Hinsley, F. H. 231 and *passim*  
 Howlett, J. 233
- Ingham, A. E. 233
- Jefferson, T. 37–9, 110, 122
- Kahn, D. 231  
 Konheim, A. G. 231, 234
- Lai, X. 187, 234  
 Lavington, S. 233  
 Leonardo of Pisa *see* Fibonacci  
 Levy, S. 234
- Massey, J. L. 187, 234  
 Metropolis, N. 233  
 Moroney, M. J. 231  
 Morse, S. 64
- Painvin, G. 58  
 Pepys, S. 7

## 236 NAME INDEX

- Piper, F. 233  
Poe, E. A. ix  
Pomerance, C. 234  
Press, W. H. 232  
Price, W. L. 233, 234  
Pujol, J. *see* GARBO
- Rabin, M. O. 212, 234  
Rivest, R. L. 171, 234  
Rota, G.-C. 233
- Scherbius, A. 111  
Shamir, A. 171, 234  
Singh, S. 234  
Solovay, R. 212, 234  
Strassen, V. 212, 234  
Stripp, A. 231 and *passim*
- Teukolsky, S. A. 232  
Tuchman, B. 231  
Turing, A. M. 161
- Vajda, S. 231  
Vallée-Poussin, C. de la 233  
Ventris, M. 7, 230  
Vetterling, W. T. 232
- Welsh, D. 230  
Wiles, A. 234  
Wittgenstein, L. 23, 230  
Wright, E. M. 232, 233  
Wright, E. V. 230
- Zimmermann, A. 65, 231  
Zimmermann, P. 187

## Subject index

- Abwehr Enigma 124, 132  
 active pins 136  
 algorithm 5  
 amplifier noise 97–8  
 anagram ix, 40  
 arithmetic, modular 10, 68, 209  
 authentication 165, 188–9  
 avalanche test (DES) 184
- Beale cipher 230  
 binary key stream 100–3  
   improving security 104–6  
 binary linear recurrence 198–202  
 birthdays paradox 191–2  
 Bletchley ix, 131, Plate 11.1  
 book cipher 36, 75–87  
   decipher table 78  
   disastrous error in using 86  
   encipher table 77  
   letter frequencies in 79, 194–5  
   solving 79–85  
 breaking ciphers 4  
 Brown corpus 23, 42  
 brute force attack 27, 44, 142, 158, 187, 215
- C36 cipher machine 133  
 C38 cipher machine 133  
 C41 cipher machine 133  
 Caesar's cipher Chapter 2 and *passim*  
 cage  
   'good' 141  
   number of 141, 206–7  
 cathode ray tube storage 161  
 cipher  
   1918 German Army 57  
   Beale 230  
   block 183  
   book *see* book cipher  
   Caesar's *see* Caesar's cipher  
   digraph-to-digraph 58  
   GARBO's *see* GARBO  
   German double Playfair 61–2  
   Japanese naval 58  
   Jefferson's cylinder 37–9  
   jigsaw *see* jigsaw cipher  
   MDTM 56  
   monograph-to-digraph 54  
   Playfair 59–60  
   simple substitution Chapter 2 and  
     *passim*  
   stencil 73–4  
   transposition Chapter 4  
   two-letter Chapter 5  
   unbreakable 36, 74  
   Vigenère Chapter 3  
 cipher system 3  
   strength of 7  
 classical sieve formula 190  
 Clipper 187  
 code 5, Chapter 6  
   error-detecting 8, 164  
   Hamming 8  
   ISBN 8  
   Italian naval 67  
   Japanese naval 67  
   Mengarini 67  
   Morse 65  
   one-part 65–6  
   two-part 66–7  
   U-boat 67  
 code-book 4  
 codebreaker 4  
 codebreaking ix, 4  
 code group 5, 38, 65  
 coin spinning 95–6  
 Colossus 159  
 combinations 207  
 combinatorics 206

## 238 SUBJECT INDEX

- computers  
 early 161  
 Manchester 161–2  
 multi-access 162  
 networks 162  
congruent 10  
continued fraction 194, 214  
core store 162  
cosmic ray 97  
coupon collector's problem 205  
crib-dragging 80  
crosswords ix  
cryptanalysis 4  
cryptanalyst 4  
cryptographer 4  
cryptographic system 3  
cryptography 4
- decipherment 3  
decryption 3  
delay line 161  
delta-ing 144  
depth 34, 93, 111, 122, 205  
 recognising 34–5  
DES 143, 169  
 chaining, use of 186  
 encipherment/decipherment 183–4  
 implementation 186  
 meet-in-the-middle attack 215  
 + RSA 186–7  
 security of 184  
 triple encipherment 185  
dice 96  
Diffie–Hellman system 166–9  
 strength of 168–9  
digraph 3  
 substitution 170  
digraph-to-digraph cipher 58  
discrete logarithm problem 168, 182  
double encipherment 52, 132  
double Playfair cipher 61–2  
double transposition cipher 44–6
- electronic mail 162  
elliptic curves 189, 215–7  
elliptic function (Weierstrass) 216  
encipher/decipher handle on Hagelin 133  
encipherment/decipherment in DES 183–4  
 definition 3  
 double 52, 132  
 on Hagelin machine 135–6  
 on SZ42 (diagram) 157  
 triple in DES 185  
 by wired wheels 116  
encryption, definition 3
- English (frequencies of letters) 18, 19  
Enigma cipher machine Chapter 9, Plates  
 9.1–9.4 and *passim*  
 Abwehr 124, 132  
 ‘Achilles heel’ 121–3  
 aligning the chains 128  
 ‘composite reflector’ 124  
 depths in messages 205  
 encipherment procedure 123  
 entry wheel 113  
 ground setting 123  
 identifying R1 128–9  
 indicator chains 125, 205  
 keyboard 112  
 modifications to 130–1  
 notch rings 112, 124, Plate 9.2  
 number of messages needed 127  
 number of trials needed 121–2  
 plugboard 121  
 reflector 113, 204  
 setting rings 112  
 wheel 112, Plates 9.1, 9.2  
 wheel motion 119  
 wheel wirings 202–4  
 Umkehrwalz *see* reflector *above*  
Eratosthenes's sieve 212  
error detecting/correcting code 8, 164  
ETH Zürich 187  
Euclidean Algorithm 177, 212–14  
Euclid's proof of infinity of primes 192–3,  
 219  
Euler's constant 205  
Euler's function 211
- factorial function 18  
factorisation 171  
Fermat–Euler Theorem 173–5, 210–11  
Fermat's ‘Last Theorem’ 173  
Fermat's ‘Little Theorem’ 173  
Fibonacci 70  
 sequence 70–1, 98, 193–4, 197–8  
FORTRAN 162  
French (frequencies of letters) 25
- Galois field 216  
‘GARBO’ (double agent) 9, 52, 88  
GARBO's ciphers 88–92  
Geiger counter 97  
German (frequencies of letters) 25  
German WW2 double Playfair cipher  
 61–3  
Greeks (ancient) 2
- Hagelin cipher machine Chapter 10,  
 Plates 10.1, 10.2 and *passim*

- active pin 136
- cage: 'good' 141; number of 141, 206–7
- decipherment 135–6
- 'delta-ing' process 144
- encipher/decipher handle 135
- encipherment 135–6
- inactive pin 136
- input wheel 135
- key value 138
- kick 135–6, 207
- lug 134–6
- lug cage 134–5
- overlapped cage 134
- overlapping 147–51
- pin 134
- pin wheel 134
- print wheel 135
- slide 147, 208; identification of 148
- solving: from cipher 150–2; from key 143–7
- unoverlapped 134
- wheel-length 134
- 'work factor' 142
- Hamming code 8
- h.c.f., finding by Euclidean Algorithm 213–14
  
- IBM 183
- IDEA 187
- identification 4
- inclusion–exclusion principle 190
- indicator 33, 86, 110, 122
- ink (secret) 9, 72
- internet Chapter 13
- ISBN code 8
- ITA (alphabet) 155–6
- Italian (frequencies of letters) 25
- Italian naval code 67
  
- Japanese 9
  - kana representation 58
- Japanese naval cipher (JN40) 58
- Japanese naval code (OTSU) 67
- Jefferson cylinder 37–9, 110, 122
- 'jigsaw' cipher Chapter 4
  
- key
  - binary 100–3
  - public Chapter 12, 171, 179
  - transposition 40
  - use of two or more 42, 46, 104–6
  - Vigenère 29
- key distribution problem 166
- key value *see* Hagelin
- keyword 59
  
- kick *see* Hagelin
- letter frequency 18, 24, 25, 79
  - in book ciphers 79, 194–5
- Linear A 230
- Linear B 7, 230
- linear congruence generator 107–9
- linear recurrence 99, 198–9, 200–2
  - cryptanalysis of 104
  - order of 99
- linear sequence
  - as key generator 101–3
  - maximum period 102–3
- Lorenz SZ42 cipher machine 106, Chapter 11
- lottery 97
- lug *see* Hagelin
- lug cage *see* Hagelin
  
- M209 cipher machine 133
- Manchester University computer 161–2
- Mariner spacecraft 8
- matrix representation of wired wheels 118
- MDTM cipher 56–8
- meet-in-the-middle attack 215
- Mengarini code 67
- microdot 9, 72
- mid-square method 106–7
- modular arithmetic 10, 68, 209
- monograph 3
- monograph-to-digraph cipher 54
- Monte Carlo method 106
- Morse code 65
- multi-access computing 162
  
- Navajo Indian language 6
- NBS (National Bureau of Standards) 183
- notch ring *see* Enigma
  
- octographic false 'hit' 31, 35
- one-part code 65–6
- one-time pad 29, 74, 92–3, 153, 195–6
- one-way function 182
- overlapping *see* Hagelin
  
- parity checking 163–4
- partition 206
- PGP ('Pretty Good Privacy') 187
- pin wheel *see* Hagelin
- Playfair cipher 59–60
  - double 61–2
  - German WW2 61–2
- plugboard *see* Enigma
- Poisson distribution 196
- Polish cryptanalysts 125–6, 128

## 240 SUBJECT INDEX

- polyalphabetic systems Chapter 3  
 polygraph 2  
 prime  
   finding large 167  
   ‘probable’ 176, 212  
 Prime Number Theorem 209  
 pseudo-random number 95, 133, 202  
 pseudo-random number generator 106  
 pseudo-random sequence 95–98  
 public key system 171, 182  
  
 random letter 95  
 random number 94–5  
 random sequence 94  
   production of 95–6  
 reflector *see* Enigma  
 repeated squaring, efficiency of 214–15  
 Rosetta stone 230  
 roulette wheel 96  
 RSA cipher 167–8, 175–82, 212–15  
   + DES 186–7  
   encipher/decipher key 175–6  
   encipher/decipher process 176  
  
 sampling with replacement 205  
 security 163  
 sequence  
   Fibonacci 70–1, 98, 193–4, 197–8  
   linear 99–103  
   pseudo-random 95–8  
   random 94–5  
 setting, cipher machine 4  
 setting ring *see* Enigma  
 sieve, classical formula 190  
 signature verification 165, 188–9  
 simple substitution cipher Chapter 2 and  
   *passim*  
   how to solve 17–19  
   minimum length for solving 16, 26  
 Skipjack, encryption algorithm 187  
 slide *see* Hagelin  
 spy Chapter 7  
 stencil cipher 73–4  
 strength of cipher system 7  
 string 3  
   length of 3  
 symbol 3  
  
 SZ42 cipher machine 106, Chapter 11  
   encipherment process 156–7  
   modification 159–60  
   wheel motion 155–6  
   work factor 158  
  
 transistor 162  
 transpositions ix, 40, 55, 74, 90  
   double 44–6, 89–92  
   irregular box 50  
   method of solution 42  
   regular box 48  
   security of 51  
   simple 40  
 trapdoor 143, 185  
 trigraph 3  
 Trojan horse attack 163  
 two-letter cipher 54  
 T52 cipher machine 154  
  
 U-boat code 67  
 Umkehrwalze *see* Enigma (reflector)  
 unbreakable cipher 29, 36, 74  
  
 Vigenère cipher 28–9, 79  
   how to solve 29, 30  
   key 29  
   text needed 37  
 Virus 163  
 Voynich Manuscript 230  
  
 Welsh (frequencies of letters) 25  
 wheels *see* Enigma, Hagelin, SZ42  
 wheel wiring *see* Enigma  
 wired wheel, encipherment by 116  
 Wittgenstein, diary of 230  
 World War 1 111  
   1918 German cipher 57, 61  
 World War 2 2, 6, 58, 67, 106, 133  
   double agent *see* GARBO  
   German double Playfair cipher 61–3  
   Italian naval cipher (Mengarini) 67  
   Japanese naval cipher (JN40) 58  
   Japanese naval code (OTSU) 67  
   U-boat code 67  
  
 Zimmermann telegram 65–6