INDEX

This is a topical index organized alphabetically. Citations are to paragraph numbers.

Alphabets. See Cipher alphabets
American standard code for information interchange. See Codes
Anagramming, 12-2
Analysis, 3-5
Aperiodic systems. See also System identification
  Depth recognition, 10-3a
  Interruptor letter, 10-1c
  Long-running key, 10-2, 10-3, 14-1g
  Polyalphabetic. See Definitions
  Solution by crib dragging, 10-3c
  Solution by depth reading, 10-3b
  Word length, 10-1a
ASCII. See Codes

Baudot. See Codes
Biliteral systems. See Definitions
  With variants. See Multiliteral with variants
Binary code, 1-5
Brute force method, 3-7, 4-10
Burst transmission, 1-7

Chaining
  Letter sequences in uniliterals, 4-8b(1)
  Linear and geometric in polyalphabetics, 9-10
Chi test
  Matching uniliteral alphabetics, 4-9e
  Periodic polyalphabetic systems, 9-7
Cipher. See Definitions
Cipher alphabets. See also Definitions
  Deciphering alphabet, 4-6b
  Direct standard alphabet, 3-2
  Enciphering alphabet, 4-6a
  Keyword mixed sequences, 4-2
  Mixed, 4-1a
  Random mixed, 4-1b
  Reconstruction of decimation mixed sequences, 4-7b, 4-8, 9-10
  Reconstruction of keyword mixed sequences, 4-7a, 4-8a
  Reconstruction of one standard sequence, 4-7
  Reconstruction of transposition mixed sequences, 4-7c, 4-8b
  Reconstruction of two mixed sequences, 4-8
  Reverse standard alphabet, 3-2
  Standard alphabet, 3-2
  Transposition mixed sequences, 4-3
  Types of, 4-5
Cipher types
  Substitution, 1-8b
  Transposition, 1-8a
Codes. See also Definitions; System identification
  ASCII, 8-2b
  Baudot, 1-5b, 8-2b
  Computer, 1-5b, 8-2
  Enciphered, 1-6, 14-1
  Morse, 1-5b, 14-1c
  Open, 14-1d
  Pamcode, 14-1d
Code systems
  Book codes, 14-2, 14-3
  Cryptography of, 14-2, 14-3
  Matrix codes and code charts, 14-3
  Solution to identification of syllabary spelling, 15-1
  Solution to the recovery of numbers, 15-3
  Solution to the recovery of syllabary spelling, 15-2
  Solution to the recovery of words and phrases, 15-4
Coincidence tests, 2-12, 2-13. See also Chi test; Delta IC; Digraphic systems; Kappa test; Phi test
Columnar transposition
  Cryptography of numerically keyed, 11-2b
  Cryptography of simple, 11-2a
  Determining matrix size, 12-1
  Exploitation, 11-1f
  Solution by anagramming, 12-2
  Solution by using hat diagrams, 12-3
  Solution of completely filled matrices, 12-1

Communications intelligence, 2-4
(CEOI). See System Operation Instructions (SOI)
Completing the plain component sequence (generatrix method), 3-7, 4-11, 9-4, 9-6b, 10-1a
Computer-based systems, 8-2
Computer code. See Codes
Computer support, 4-9b, F-1 through F-3
Chi test for mixed alphabet periodics, 9-7c
Frequency matching in periodic systems, 9-3
Generatrix method for periodics, 9-4
Kappa test, 10-3a(3)
Periodic polyalphabetics, 8-4a, 8-4c
Concealment systems, 1-7
Consonant line, 4-13
Crib dragging, 9-2, 10-3c
Cross IC. See Chi test
Cryptanalysis basic steps, 2-6
Cryptogram, 1-2
Cryptographer, 1-2
Cryptographic systems
Ciphers, 1-5
Codes, 1-5
Deciphering alphabet, 4-6b
Definitions
Aperiodic polyalphabetic, 8-1
Biliteral, 5-2
Cipher, 1-5
Cipher alphabets, 1-9
Code, 1-5
Cryptography, 1-3, 3-3
Cryptology, 1-1
Delta IC, 2-14g. See also Digraphic systems
Digraphic systems, 6-7
Dinomic systems, 5-2
Four-square systems, 6-3a
Isologs, 5-12
Keyword mixed sequence, 4-2
Monoalphabetic, 3-1
Monoalphabetic uniliteral substitution, 3-1
Monographic, 3-1
Monome-dinome systems, 5-2
Multiliteral substitution, 5-1
Periodic systems, 9-1
Plaintext, 1-5
Polyalphabetic systems, 3-1c
Polygraphic systems, 3-1c, 6-1
Substitution, 1-8b
Syllabary squares, 5-2
Transposition, 1-8a
Transposition mixed sequence, 4-3
Triliteral and trinomic systems, 5-2
Delta IC, 2-14g, 8-4
Depth, 10-3
Diagnostics. See System identification
Digraphic systems. See also Definitions; Four-square systems; Playfair systems; System identificatiion; Two-square systems
Cryptography of large table systems, 6-2
IC, 6-9
Phi test, 6-9
Substitution matrix, 6-2
Word patterns, 7-1, 7-2
Dinomic systems. See Definitions
With variants. See Multiliteral with variants
Direct symmetry, 9-8
Discriminants. See Specific keys
ETNROAIS, 2-8, 2-9
Encipher below, decipher above (EBDA), 6-6, 7-5, 7-6
Encipher right, decipher left (ERDL), 6-6, 7-5, 7-6
Enciphered alphabet. See Cipher alphabets
Enciphered codes. See Codes
Encryption, 1-2, 1-5
External variant systems. See Multiliteral with variants
Factoring, 8-3
Flush depth, 10-3
Four-square systems. See also Definitions
Cryptography of, 6-3
Mixed four-squares, 7-3
Regular four-squares, 7-2
Frequency counts
Analysis by, 9-3
Consonant line, 4-13a(4)
Digraphic, 6-8, 6-10
Dinomic, 5-6
Monome-dinome, 5-7
Periodic polyalphabetic systems, 8-4
Triliteral, 4-13b
Uniliteral, 4-9
Frequency distribution, 2-9, 2-10
Frequency matching. See also Chi test
Uniliteral systems, 3-6
Variant multiliteral systems, 5-11
Generatrix method. See Completing the plain component sequence
Geometric chaining. See Chaining
Hat diagrams, 12-3
Hexadecimal arithmetic, 8-2b
Highs and lows. See Peaks and troughs
Horizontal two-square. See Two-square systems
IC. See Coincidence tests
Idiomorphs. See Word patterns
Index of coincidence. See Coincidence tests
Indicator systems, 2-6b, 3-3b, 14-12a(2), 10-3a

Indirect symmetry, 9-9, 9-10
Internal variant systems. See Multiliteral with variants
Interruptor letter aperiodics, 10-1c
Isologous segements, 5-13, 5-15
Isologs. See also Definitions
  Analysis of, 7-1
  In periodic polyalphabetics, 9-11
  In Playfair systems, 6-10b
  In syllabary squares, 5-15
  In variant systems, 5-12

Kappa test, 10-3a(3)
Keyword mixed sequence. See also Definitions
  In biliteral and dinomic systems, 5-6
  Completing the plain component, 3-7, 4-11, 9-6
  In four-square systems, 6-3, 7-2, 7-3
  In monome-dinome systems, 5-7
  In periodic systems, 9-7
  In Playfair systems, 7-6
  In two-square systems, 6-4, 6-5

Language characteristics, 2-8, 2-9, 2-11 through 2-13, 4-13, 15-4
Letter frequencies, 2-9, 2-10
Linear chaining, 9-10
Logarithmic weights of letter probabilities, 9-4e
Long-running key aperiodics. See Aperiodic systems
Low frequency letters
  For fillers, 3-4c, 3-6d, 6-10b(7)
  JKQXZ, 2-8a
  For nulls, 6-6e, 6-10b(7)

Machine systems, 8-2
Matrices
  Analyst's, 9-9, 9-10, 12-3
  Code chart, 14-3
  Columnar transposition, 11-2
  Completely filled, 11-2, 12-1
  Coordinate matrix systems, 5-3
  Incompletely filled, 11-2, 12-3
  For transposition mixed sequences, 4-3
Message
  Externals, 2-5
  For messages in depth. See Depth
  Preparation, 3-4
Microdots, 1-7
Mixed cipher alphabets, 4-1
Modulo arithmetic, 5-3f, 8-1e
Monoalphabetic multiliteral systems. See Multiliteral systems
Monoalphabetic uniliteral substitution. See Definitions; Uniliteral systems
Monographic. See Definitions; Phi tests
Monome-dinome systems. See also Definitions; System identification
  Cryptography of, 5-3
  Solution of, 5-7
Multiliteral substitution. See Definitions; Monome-dinome systems; Syllabary squares; Triliteral and trinomic systems
Multiliteral systems. See also System identification
  Analysis techniques, 5-4
  Cryptology of simple, 5-3
  Solution by vowel-consonant relationships, 5-8
  Solution of dinomic and biliteral systems of simple, 5-6
  Solution of isologous segments, 5-13
  Solution of isologs, 5-12
  With variants, solution of external variant systems, 5-11
  With variants, solution of internal variant systems, 5-14

Nonrepeating key, 8-1c. See also Aperiodic systems
Numerically-keyed aperiodics. See Aperiodic systems
Numerically-keyed columnar transposition. See Columnar transposition

Offset depth, 10-3
One-time pad system, 10-2

Pamcodes. See Codes
Peaks and troughs, 2-11, 2-15, 3-6, 4-9d, 6-7e, 8-3, 8-4, 9-3
Periodic polyalphabetic systems. See Periodic systems
Periodic systems. See also Definitions
  Accidental repeats in, 8-3, 8-4
  Determining the period length, 8-3, 8-4
  Factoring, 8-3
  IC, 8-4
  Solution of mixed alphabets by linear and geometric chaining, 9-10
  Solution of mixed alphabets by the chi test, 9-7c
  Solution of mixed alphabets in, 9-5
  Solution of mixed alphabets in direct symmetry, 9-8
  Solution of mixed alphabets in indirect symmetry, 9-9, 9-10
  Solution of mixed alphabets in isologs, 9-11
  Solution of mixed alphabets when both sequences are known, 9-6
  Solution of mixed alphabets with known plaintext sequences, 9-8
  Solution of mixed alphabets with unknown mixed sequences, 9-9
  Solution of standard alphabets by frequency matching, 9-3
  Solution of standard alphabets by the generatrix method, 9-4
  Solution of standard alphabets by the probable word method, 9-2
  Solution of standard alphabets in, 9-1
Phi test. See also Digraphic systems
  Calculation, 2-14
  Interpretation, 2-15

Playfair systems. See also System identification
Cryptography of, 6-6
Solution of digraphic word patterns in, 7-5
Solution of matrix reconstruction in, 7-6
Polyalphabetic systems. See also Aperiodic systems; Definitions; Periodic systems; System identification
Baudot code. See Codes
Machine and computer based systems, 8-2
Types, 8-1
Polygraphic. See Definitions; Digraphic systems; Four-square systems; Playfair systems; Two-square systems
Prearranged message codes. See Codes
Probable word method, 4-10, 4-12
Pseudotext, 3-7, 4-10, 4-11, 5-11
Rectangular rule, 6-3 through 6-5, 7-5, 7-6
Repeating keys, 8-1, 9-11, 14-1
Repeats, 4-9, 8-4
Roughness, 2-11
Route transposition, 11-1, 11-3
Sequence
Decimation mixed, 4-4
Direct standard, 3-2
Keyword mixed, 4-2
Random mixed, 4-1
Reverse standard, 3-2
Standard, 3-2
Tranposition mixed, 4-3
Signal communications, 1-4
Signal Operation Instructions (SOI), 3-3a
Specific keys, 2-6b, 3-3
Standard sequence. See Sequence
Statistical tests. See Coincidence tests
Stereotypes, 4-12
Sum checks, 5-3f
Superencipherment, 1-6
Superencryption, 1-6
Syllabary spelling. See Code systems
Syllabary squares. See also Definitions
Cryptography of, 5-3e
Solution of, 5-15
System identification
Chi test (cross IC), 4-9e, 9-7
Coincidence tests, 2-12
Delta IC, 2-14g, 8-4
Delta IC with periodic systems, 8-4
Digraphic systems, 6-7, 6-9, 6-10
Extended examples, 6-10
Grouping messages by system for, 4-9
Index of coincidence, 2-13
Kappa test, 10-3a(3)
Letter frequencies, 2-10
Monographic phi test, 2-14
Monome-dinome systems, 5-7
Multiliteral systems, simple, 5-5
Multiliteral systems with variants, 5-10
Phi test interpretation, 2-15
Playfair systems, 6-7d, 6-9, 6-10
Polyalphabetic systems, 2-10c, 8-3
Roughness, 2-11
Transposition systems, 2-10a, 11-1
Two-square systems, 6-10, 7-4
System indicators, 2-6b, 3-3
System requirements, 2-1
Tests. See Coincidence tests
Traffic analysis, 2-5
Transparencies
Direct, 6-4b, 6-5b, 6-7c, 7-4
Reverse, 6-5b, 6-7c, 7-4
Transposition, columnar. See Columnar transposition
Transposition mixed sequence
Numerically-keyed columnar, 4-3b, 4-7d
Recovery of, 4-7c
Simple columnar, 4-3a
Transposition, route. See Route transposition
Transposition systems. See also System identification
Geometric process, 11-1c
Grille, 11-1d
Solution of messages with similar beginnings and endings, 13-2
Solution of messages with the same length and keys, 13-3
Solution of special exploitable situations, 13-1
Trial decipherment
Using the brute force method, 3-7, 4-10, 4-11
For variant multiliteral systems, 5-11
Triliteral and trinomic systems. See also Defintions
Cryptography of, 5-3b
Solution of, 5-9
Triliteral frequency counts, 4-13b
Two-square systems. See also System identification
Cryptography of, 6-4, 6-5
Solution of, 6-4b, 7-4
Uniliteral systems
Frequency distribution, 2-9
Preparation for analysis, 4-9
Solution by completing the plain component sequence, 3-7, 4-11
Solution by frequency matching, 3-6, 4-10
Solution by the brute force method, 3-7, 4-10, 4-11
Solution by the generatrix method, 3-7, 4-11
Solution by the probable word method, 4-10, 4-12
Solution by using vowel-consonant relationships, 4-13
Solution with computer support, 4-9
Stereotypes, 4-13
Word patterns (idiomorphs), 4-12c
Worksheet preparation, 4-9

Variant systems. See Multiliteral with variants
Vertical two-square. See Two-square systems
Vigenere square, 8-1, 10-3
Vowel-consonant relationships
Consonant line, 4-13
In multiliteral systems, 5-8
In uniliteral systems, 4-13
Word patterns (idiomorphs), 4-12c, 5-6d, 5-6e, 5-7d, 7-1 through 7-3, 7-5, 7-6, 15-2
Word-length aperiodics. See Aperiodic systems
Worksheet preparation, 4-9