Introducción.

Capítulo I — Generalidades y terminología.

1. Las dos partes de la criptografía.
2. Generalidades sobre el cifrado.
3. Clasificación de los métodos y procesos de cifrado.
4. Sistemas de cifrado.
5. Reglas generales de la ciencia del cifrado.
6. Generalidades sobre criptoanálisis.
7. Casos en los que el problema del criptoanálisis está completo. Capacidad de cifrado perfecto.
8. Circunstancias que pueden facilitar el criptoanálisis.
9. Información procedente de indicadores. Cifrado perfecto aparente y cifrado perfecto real.
10. Información sobre el modo de cifrado.
11. Fallos sistemáticos del cifrado.
12. Importancia de la teoría y conclusión.

Capítulo II — Características de la lengua francesa.

13. Características de un idioma. Definición de frecuencia.
14. Frecuencias de letras en francés.
15. Características de las letras deducidas de la frecuencia de ciertos bigramas.
16. Tabla de frecuencias de letras duplicadas.
17. Otros bigramas característicos de ciertas letras.
18. Frecuencias de bigramas.
19. Frecuencias de trigramas.
20. Frecuencia de las palabras. Consideraciones finales.

Parte Primera.

Transposiciones puras.

Capítulo I — Estudio general de las transposiciones puras.

1. Antigüedad de los métodos de transposición. Sus definiciones.
2. Característica general de las transposiciones puras.
3. Secuencia criptográfica y secuela del anagrama.
4. Método general para el criptoanálisis de transposiciones.
5. Ejemplo de criptoanálisis mediante el método general.
6. Caso de dos criptogramas de la misma longitud y de la misma clave.
7. Método general usando palabras probables.
8. Otras generalidades en transposiciones.
9. Accidentes y fallos de cifrado.
10. Capacidad de cifrado perfecta de las transposiciones. Valor criptográfico de esta categoría de procedimientos.

Capítulo II — Transposición sencilla ordinaria con tablas.

11. Clave de Transposición.
12. Cifrado y descifrado.
13. Observación sobre la disposición de la llave.
14. Estudio de la secuencia XP.
15. Criptoanálisis.
16. Caso de una tabla completa.
17. Método del sombrero. Caso de una tabla casi completa.
18. Ejemplo de criptoanálisis de una tabla casi completa.
19. Caso general de una tabla absolutamente arbitraria.
20. Ejemplo de criptoanálisis analítico.
21. Continuación del criptoanálisis analítico.
22. Ejemplo de criptoanálisis usando una palabra probable.
23. Otros métodos de usar una palabra probable.
24. Métodos empíricos.
25. Casos particulares. Accidentes de cifrado.
26. Ejemplos de criptoanálisis según diversos accidentes de cifrado.
    a) Las dos claves son diferentes y no tienen la misma longitud.
    b) Las dos claves son diferentes, pero tienen la misma longitud.
    c) Los dos mensajes fueron cifrados con la misma clave.
27. Reconstrucción de una clave de texto plano literal.
28. Observación sobre la posibilidad teórica de utilizar la numeración de la clave para facilitar el criptoanálisis.
29. Interés práctico del estudio de las transposiciones simples.

Capítulo III — Transposiciones simples mejoradas.

30. Posible mejora de la transposición simple ordinaria.
31. Lectura alternada de las columnas de arriba a abajo y de abajo a arriba.
32. Extracción diagonal.
33. Tablas completas irregulares.
34. Transposiciones de tablas simples mejoradas con agujeros.
35. Varias posible soluciones.
36. Desciframiento de transposiciones simples mejoradas.
37. Doble transposición.
38. Uso de un texto clave. Tablas con celdas numeradas.
39. Secuencias criptográficas fragmentadas.
40. Otros procesos de transposición simple. Variante de Richelieu. Método del coronel Roche.
41. Procedimiento de Porta.

Capítulo IV — Transposición simple de rejilla.

42. Definición de la rejilla.
43. Varios tipos de rejillas.
44. Rejillas giratorias cuadradas. Modos de uso clásicos (con cuadrados completos).
45. Criptoanálisis de cuadrículas utilizadas con cuadrados completos.
46. Ejemplos de criptoanálisis.
47. Modos de uso racional de las rejillas giratorias.

48. Ventajas comparativas de cada uno de los dos modos de uso.
49. Uso de una contrarejilla.
50. Seguridad criptográfica finalmente obtenida.
51. Método de formación y número de rejillas de giro cuadradas.
52. Otros tipos de rejillas con ventanas cuadradas.
53. Rejillas indefinidas.

Capítulo V. Doble transposición.

54. Definición y diversas categorías.
55. Diferentes casos de doble transposición realizada por dos tablas completas. Primer caso: p_1 es un múltiplo de n_2 .
56. Segundo caso: p_1 es un submúltiplo de n_2.
57. Tercer caso general: ¿p_1 dividido por n_2 es igual a a dividido por b.
58. Principio de criptoanálisis
59. Ejemplo de criptoanálisis
60. Caso especial de dos transposiciones simples sucesivas realizadas con la misma clave.
61. Caso de tablas incompletas. Capacidad de cifrado perfecto real
62. Otras posibilidades de criptoanálisis: errores y fallos de cifrado.
63. Reconstrucción de claves numéricas a partir de una secuencia XP.
64. Ejemplo de reconstrucción de clave numérica.
65. Caso general de dos transposiciones cualesquiera.
66. Conclusiones sobre la doble transposición y sobre la transposición en general.

SEGUNDA PARTE.

Sustituciones puras.

Capítulo I — Definición de claves de sustitución. Sustitución alfabetos.

1. Antigüedad de los procedimientos de sustitución.
2. Claves de sustitución. Definición de una clave simple.
3. Valor criptográfico de una clave simple.
4. Comodidad de uso de claves simples. Importancia fundamental de las claves simples literales.
5. Sustituciones inversas. Alfabetos inversos. Alfabetos recíprocos.
6. Familias de alfabetos. Alfabetos clásicos ordenados normalmente.
7. Alfabetos complementarios. Sustitución complementaria.
8. Alfabetos normalmente paralelos. Alfabetos no normalmente paralelos. Alfabetos no paralelos.
9. Alfabetos inversos de una familia de alfabetos paralelos.
10. Alfabetos semiordenados. Alfabetos invertidos. Alfabetos superpuestos.
11. Método para formar alfabetos superpuestos a partir de un alfabeto original.
12. Alfabetos desordenados incoherentes.
13. Métodos de formación simples y clásicos según una palabra clave.
14. Críticas ya formuladas y otros métodos de formación propuestos por diversos autores.
15. Otros tipos de claves simples. Cuadrado de cifrado (de 25).
16. Sustitución de doble clave. Definición.
17. Clasificación de las sustituciones puras.

Capítulo II — Sustituciones simples ordinarias.

18. Características de las sustituciones simples ordinarias.
19. Sustituciones simples clásicas (por alfabetos ordenados normalmente).
20. Criptoanálisis de sustituciones simples ordinarias.
21. Ejemplo de criptoanálisis mediante el método analítico.
22. Criptoanálisis mediante el método de la palabra probable.
23. Valor de una palabra probable en la sustitución simple ordinaria. Capacidad de cifrado perfecto real.
24. Ejemplo de reconstrucción de un alfabeto de sustitución establecido según el método de formación clásico.
25. Método de criptoanálisis mediante búsqueda por palabras clave.
26. Uso práctico de secuencias numéricas para el estudio.
27. Ejemplo de criptoanálisis mediante el método de palabras clave.
28. Criptoanálisis de sustituciones simples ordinarias de otro tipo.
29. Últimos tipos de sustituciones simples ordinarias. La alternativa económica de Delastelle. Método general de criptoanálisis

Capítulo III. - Sustituciones simples con múltiples representaciones.

30. Generalidades sobre sustituciones literales simples con múltiples representaciones.
31. Dos categorías de sustituciones simples con múltiples representaciones.
32. Uso de un cuadrado de cifrado.
33. Crítica de estos métodos.
34. Otros métodos de sustitución con múltiples representaciones.
35. Otros inconvenientes de las sustituciones simples con múltiples representaciones.

Capítulo IV. - Sustituciones simples con bigramas.

36. Generalidades sobre sustituciones simples por bigramas.
37. Equivalencia con dos sustituciones literales simples.
38. Ejemplos de errores de cifrado sistemáticos.
39. Procedimientos de sustitución bigramática utilizados en la práctica.
    1. Uso de listas o tablas.
    2. Tableros de ajedrez bigramáticos de Delastelle.
    3. Método de Playfair,
40. Criptoanálisis. El caso de Playfair.
41. Posibilidades de criptoanálisis utilizando una palabra probable o la palabra clave del cuadrado cifrado.
42. Ejemplo de criptoanálisis.
43. Criptoanálisis en el caso general.
44. Sustitución bigramática utilizando alfabetos bífidos de Delastelle.
45. Sustituciones por poligramas. Alfabetos trífidos. Conclusión.

Capítulo V. - Generalidades sobre el cifrado de doble clave. Definición. Orígenes históricos.

46. Definición de la verdadera sustitución de doble clave.
47. Vigenère, inventor de la sustitución de doble clave.
48. Los precursores de Vigenère:
    1. Tritemio.
    2. Gabriel De Collange.

49. Bellaso.
50. Porta.
51. Vigenère.
52. Últimas mejoras en la sustitución de doble clave:
    1. Variaciones clásicas (por alfabetos ordenados normalmente)
    2. Variaciones empleando alfabetos secretos desordenados.
53. Características generales de las sustituciones de doble clave.
54. Método general de criptoanálisis.

Capítulo VI. - Sustituciones de doble clave clásicas. Generalidades.

55. Definición de sustituciones clásicas de doble clave.
56. Variantes del principio :
    1. Modo de cifrado según Vigenère.
    2. Variante de Beaufort .
    3. Variante alemana.
57. Ecuaciones de cifrado.
58. Otras formas del cuadro clásico:
    1. Cuadro con alfabetos desplazados de izquierda a derecha.
    2. Cuadro con letras ordenadas en dirección opuesta.
59. Segunda variante del cifrado alemán.
60. Uso de un desplazamiento constante adicional.
61. Regletas clásicas de dimensión reducida.

Capítulo VII. - Sustitución de doble clave clásicas. Variantes de Porta y Gronsfeld.

62. Variante de Porta.
63. Ejemplo de criptoanálisis utilizando el método analítico.
64. Criptoanálisis mediante el método de la palabra probable.
65. Tablas de búsqueda de palabras probables y palabras clave.
66. Otro método de palabra probable.
67. Variante de Gronsfeld.

Capítulo VIII. - Otras variantes de aplicación de la clave.

68. Cambio de clave durante el cifrado.
69. Uso de letras nulas.
70. Método de clave interrumpido:
    1. Uso de una letra de parada.
    2. Uso de una convención adicional.
71. Clave desperiodizada por agujeros.
72. Clave en claro indefinida.
73. Cifrados por autoclave.
74. Método de criptoanálisis del Comandante Bassières.
75. Regreso a una clave periódica ordinaria.
76. Autoclaves con el texto criptográfico como clave. Métodos de autocifrado.
77. Clave maestra cíclica. Discos.
78. Criptoanálisis mediante el método del comandante Bassières.
79. Variantes de alta seguridad. Variante de General Sacco.
80. Variante de Rozier.

Capítulo IX. - Otras variantes de cifrado de doble clave. Generalidades sobre el criptoanálisis de las sustituciones de clave doble mediante alfabetos desordenados:

81. Cifrado por tramos. El criptógrafo de Alberti.
82. Instrumentos para cifrar con alfabetos normalmente paralelos.
83. Instrumentos de cifrado que utilizan alfabetos no normalmente paralelos.
84. Facilidad de uso. Tablas inversas. Tabla reversible de Delastelle.
85. Regletas inversas establecidas con la ayuda de alfabetos superpuestos.
86. Alfabetos verdaderamente no paralelos.
87. Uso de alfabetos independientes.
88. Generalidades sobre el criptoanálisis de sustituciones de doble clave utilizando alfabetos secretos desordenados.

Capítulo X. Criptoanálisis de sustituciones de doble clave mediante alfabetos secretos desordenados

89. Caso de alfabetos normalmente paralelos. Principio general de estudio.
90. Ejemplo de criptoanálisis en el caso de una clave periódica ordinaria.
91. Determinación de la longitud de la clave periódica. Frecuencias.
92. Uso de una palabra probable.
93. Uso del paralelismo normal y de la palabra clave principal.
94. Fin del criptoanálisis mediante la búsqueda de la palabra clave del alfabeto secreto del deslizador.
95. Uso de secuencias numéricas de estudio.
96. Caso de otras variantes de aplicación de la clave. Discos con un alfabeto secreto. Autoclaves.
97. Caso de alfabetos no normalmente paralelos. Uso del paralelismo vertical.
98. Ejemplo del uso del paralelismo horizontal en un caso particular
    a) Determinación de la longitud de la clave principal.
    b) Regla ficticia de estudio.
    c) Uso de una palabra probable

99. Reconstrucción de un instrumento de cifrado gracias al paralelismo no normal.
100. Ejemplo concreto de dicha reconstrucción.
101. Caso de un instrumento de cifrado conocido.
102. Caso de alfabetos independendientes.

Capítulo XI — Criptógrafos y máquinas de cifrado

103. Aparatos diversos. Criptógrafo de Wheatstone.
104. Criptografo de Bazeries
105. Criptografo de Ducros.
106. Criptografos de barras verticales móviles.
107. Criptógrafos portátiles y máquinas de cifrado Hagelin
108. Máquina Enigma alemana. Modelo teórico descrito por Givierge.
109. Implementación real de la Enigma
110. Tomógrafos. Modelo Hagelin de dos canales.
111. Teletipos cifradores de cinco impulsos.
112. Construcción del primer tipo.
113. Teleimpresora cifradora de Siemens

114. Otras máquinas de cifrado
115. Conclusiones sobre las sustituciones puras y sobre las máquinas de cifrado.

TERCERA PARTE

Métodos combinados — Métodos de código

Medios auxiliares de cifrado

Nota preliminar a la tercera parte

Capítulo I. Sustitución y transposición simples

1. Varios categorías de métodos combinados.

A. métodos combinados ordinarios.

2. Sustitución simple y transposición
3. Transposición y sustitución con doble clave.
    1. Transposición y sustitución con doble clave.
    2. Sustitución con doble clave y transposición.
4. Presentación de un método particular de criptoanálisis (M. Painvin).
5. Caso general. Elección racional de tales combinaciones.

B. Métodos Tomográmicos.

6. Sustitución simple de letras en bigramas y transposición.
7. Ejemplo histórico de criptoanálisis.
8. Otro método tomográmico.

C. Métodos complejos.

9. Procedimientos complejos de Delastelle.
10. Sustituciones migramáticas.
11. Otro procedimientos complejos.
12. Principio del criptoanálisis de métodos complejos

Capítulo II. Sustituciones de códigos.

A. Cifrado simple

13. Cifrado simple. Documentos codificados diversos.
14. Capacidad teórica y riqueza efectiva de un código
15. Función criptográfica y función abreviada de los códigos
16. Influencia de otras características de la composición y de los hábitos de los cifradores en el valor de un código.
17. Criptoanálisis en el caso general.
18. Grupos de silabas, grupos característicos.
19. Consejos generales y propósito del criptoanálisis.

13. Probabilidad de las causas, fórmula de Bayes.

C. Ejemplos sencillos de aplicación de cálculos de probabilidad en criptografía

1. Utilidad de dichos cálculos. Su valor y su precisión.
2. Probabilidades unitarias en criptografía.
3. Caso de las unidades de cifrado.
4. Caso de los grupos en códigos.
5. Problema de las repeticiones.
6. Fórmula de Newton.
7. Primera aplicación práctica: caso en el que se aplica la ley de los grandes números.
8. Segundo problema práctico: probabilidad de un número determinado de letras "e" en un texto plano.
9. Tercer problema práctico: probabilidad de que la letra e sea la más frecuente.
10. Probabilidad de las frecuencias de una transposición.
11. Probabilidad de las frecuencias de una sustitución simple.
12. Caso de sustituciones de doble clave.
13. Problema especial: estudio del valor de un criterio.
14. Caso de códigos. Conclusiones.

Apéndice n.º 2. Una teoría matemática de los sistemas de cifrado (Shannon).

1. Referencias y limitaciones del presente estudio.
2. Fundamentos generales de las teorías de Shannon.
3. Estructura matemática de una fuente de información. Entropía. Redundancia. Equivocación.
4. Teoría de las telecomunicaciones.
5. El álgebra de los sistemas de cifrado.
6. Secreto teórico. Secreto práctico. Discusión.
7. Condiciones matemáticas del secreto perfecto.
8. Equivocación en el caso general. Sistemas ideales.
9. Características del trabajo y secreto práctico. Conclusiones,

Apéndice n.º 3. Características estadísticas de la lengua rusa.

Apéndice n.º 4. Características estadísticas de la lengua alemana.

Apéndice n.º 5. Características estadísticas del idioma inglés.

Apéndice nº 6. Características estadísticas de la lengua española.

Apéndice nº 7. Características estadísticas de la lengua italiana.

Tabla de frecuencias de bigramas en francés: fuera del texto, al final.

Tabla de frecuencias de bigramas en ruso: fuera del texto, al final.