

LA ESCRITURA SECRETA

A continuación tienes un examen de estudio basado en la obra *Codes and Ciphers: Secret Writing Through the Ages*, de John Laffin. He formulado preguntas que abarcan las definiciones, los sistemas históricos, la transmisión secreta y el criptoanálisis. Después de cada pregunta aparece una respuesta completa.

1. ¿Qué es la criptografía?

La criptografía es el arte o la técnica de enviar un mensaje de manera que su significado quede oculto para todas las personas excepto para el emisor y el destinatario autorizado.

La palabra procede de los términos griegos *kryptos*, que significa “secreto”, y *graphos*, que significa “escritura”. Por tanto, la criptografía puede definirse como la escritura secreta.

Su finalidad principal es proteger la confidencialidad de una comunicación. Sin embargo, la existencia de un mensaje cifrado también puede despertar el interés de los adversarios, que intentarán interceptarlo y descifrarlo.

2. ¿Cuál es la diferencia entre código y cifrado?

Un **código** es un sistema previamente acordado en el que una palabra, número o expresión representa otra palabra, varias palabras o incluso un mensaje completo.

Por ejemplo, una palabra como “agape” podía significar “abandonar las negociaciones”. Para comprender un código normalmente es necesario disponer de un libro o diccionario de códigos.

Un **cifrado**, en cambio, transforma sistemáticamente los elementos del mensaje original. Las letras pueden sustituirse por otras letras, números o símbolos, o pueden cambiar de posición.

La diferencia fundamental es la siguiente:

Código	Cifrado
Una palabra puede representar una frase completa.	Se transforman normalmente las letras o unidades del mensaje.
Necesita un código o diccionario.	Puede descifrarse conociendo la clave y el procedimiento.
Tiene un vocabulario limitado.	Puede expresar cualquier pensamiento.
Cambiarlo exige preparar nuevos libros de códigos.	Puede cambiarse rápidamente modificando la clave.

Morse suele llamarse “código Morse”, pero técnicamente es un **cifrado o sistema de representación**, porque cada letra se representa mediante una combinación de puntos y rayas, no mediante palabras que sustituyan frases completas.

3. ¿Qué es un mensaje en claro?

El mensaje en claro es el texto original antes de aplicarle un código o un cifrado.

Por ejemplo:

ATAQUE AL AMANECER

Antes de ser transformado, ese mensaje constituye el texto claro o mensaje original.

Después de aplicar una operación criptográfica, se obtiene el **criptograma**, que es el texto aparentemente incomprensible que debe analizarse para recuperar el mensaje en claro.

4. ¿Qué es una clave?

La clave es el elemento secreto que permite aplicar o invertir un sistema de cifrado.

En algunos sistemas la clave puede ser una palabra, una letra, un número, una disposición geométrica o una tabla. Por ejemplo, en el cifrado de Vigenère puede utilizarse la palabra **SAFE**.

El sistema de cifrado puede ser conocido por varias personas, pero sin la clave correcta el adversario tendrá más dificultades para recuperar el mensaje.

La arquitectura básica es:

Mensaje → cifrado → transmisión → interceptación → análisis → descifrado

5. ¿Cuáles son los dos principios fundamentales de los cifrados?

Los dos principios fundamentales son:

1. **Sustitución.**
2. **Transposición.**

También pueden combinarse ambos procedimientos para crear un cifrado más complejo.

6. ¿Qué es una sustitución?

En una sustitución, cada letra, número o símbolo del mensaje original se reemplaza por otro elemento.

Por ejemplo, si cada letra se sustituye por la letra anterior del alfabeto:

- A se convierte en Z.
- B se convierte en A.
- C se convierte en B.

El mensaje:

STAY AWAY

podría convertirse en:

RSZX ZVZX

Las letras cambian, pero normalmente conservan sus posiciones relativas.

Una sustitución sencilla puede descubrirse mediante el análisis de frecuencias, porque una misma letra del texto original suele transformarse siempre en el mismo símbolo.

7. ¿Qué es una transposición?

En una transposición, las letras del mensaje permanecen iguales, pero se cambia su orden o posición.

Por ejemplo, la frase:

MEET YOU AT FOUR

podría escribirse al revés por palabras:

TEEM UOY TA RUOF

La característica principal de una transposición es que conserva las letras del mensaje original. Por eso, si se analizan sus frecuencias, estas pueden seguir siendo parecidas a las del idioma original, aunque el mensaje sea difícil de leer.

8. ¿Qué diferencia existe entre sustitución y transposición?

En la sustitución se modifica la identidad o representación de las letras.

En la transposición se modifica la posición de las letras.

Ejemplo:

- Mensaje original: ATAQUE
- Sustitución: DWDTXH
- Transposición: EQAUTA

En el primer caso las letras han sido cambiadas. En el segundo, las letras originales siguen presentes, pero aparecen desordenadas.

9. ¿Qué es una combinación de sustitución y transposición?

Es un procedimiento que aplica las dos operaciones sucesivamente.

Primero se pueden sustituir las letras del mensaje y después cambiar su orden, o realizar primero la transposición y posteriormente la sustitución.

La combinación aumenta la dificultad porque el analista debe descubrir dos estructuras:

- Qué transformación se aplicó a las letras.
- Qué orden se utilizó para reorganizarlas.

10. ¿En qué consiste el cifrado de César?

El cifrado de César es una sustitución en la que cada letra se desplaza un número fijo de posiciones en el alfabeto.

Julio César utilizaba un desplazamiento de tres lugares. Por ejemplo:

- A se convierte en D.
- B se convierte en E.

- C se convierte en F.

La palabra:

ATTACK

se transforma en:

DWWDFN

Es un sistema sencillo y actualmente inseguro porque solo existen pocas posibilidades de desplazamiento. Un analista puede probar todos los desplazamientos posibles.

11. ¿Por qué el cifrado de César es débil?

Es débil por varias razones:

- Utiliza una sustitución fija.
- Cada letra siempre se transforma de la misma manera.
- Conserva las frecuencias relativas de las letras.
- El número de claves posibles es muy reducido.
- Puede resolverse probando todos los desplazamientos.

Por ejemplo, si una letra aparece con mucha frecuencia en el criptograma, probablemente corresponda a la letra más frecuente del idioma, como la E en inglés.

12. ¿Qué era la escítala?

La escítala era un sistema de transposición utilizado en la antigua Grecia, especialmente asociado a los espartanos.

Consistía en una tira de cuero o pergamino enrollada alrededor de un bastón cilíndrico. El mensaje se escribía a lo largo del cilindro. Al desenrollar la tira, las letras quedaban aparentemente desordenadas.

El destinatario necesitaba un bastón de igual diámetro para volver a enrollar la tira y leer el mensaje.

La clave, en este caso, era esencialmente el tamaño o diámetro del bastón.

13. ¿Por qué la escítala es un sistema de transposición?

Porque las letras del mensaje no se sustituyen por otras. Se mantienen las mismas letras, pero se reorganizan debido a la forma en que se escriben alrededor del bastón.

Su estructura puede resumirse así:

1. Se prepara una tira larga.
2. Se enrolla alrededor de un cilindro.
3. Se escribe el mensaje siguiendo la superficie del cilindro.
4. Se desenrolla la tira.

5. El receptor la vuelve a enrollar sobre un cilindro del mismo tamaño.

14. ¿Qué era el alfabeto zodiacal?

El alfabeto zodiacal era un sistema simbólico en el que cada letra se representaba mediante un signo relacionado con los planetas, las constelaciones u otros símbolos astrológicos.

Su principal característica era ocultar el aspecto normal de la escritura. Una persona que no conociera la equivalencia podía pensar que se trataba de un texto astrológico o mágico.

Era principalmente una sustitución simbólica:

- La letra original se sustituía por un signo.
- El receptor necesitaba conocer la tabla de equivalencias.

15. ¿Quién fue Trithemius y cuál fue su importancia?

Johannes Trithemius fue un abad benedictino alemán que escribió *Polygraphia*, considerada una de las primeras obras importantes sobre criptografía.

Su sistema utilizaba varios alfabetos y permitía sustituir las letras por palabras o frases. Por ejemplo, una letra podía representarse mediante expresiones relacionadas con la eternidad, la divinidad o el reino de Dios.

Su método tenía algunas ventajas:

- Podía ocultar incluso la existencia de un mensaje cifrado.
- Permitía emplear frases aparentemente normales.
- Una misma letra podía tener varios equivalentes.
- El análisis resultaba más difícil porque no existía una única sustitución evidente.

Su principal desventaja era que resultaba lento y laborioso para mensajes largos.

16. ¿Qué era la rejilla de Cardano?

La rejilla de Cardano era un sistema de escritura secreta basado en una hoja con agujeros o ventanas.

El procedimiento era el siguiente:

1. Se colocaba la rejilla sobre una hoja.
2. Se escribía el mensaje secreto a través de los agujeros.
3. Se retiraba la rejilla.
4. Se redactaba un texto aparentemente normal alrededor de las letras secretas.
5. El destinatario colocaba otra rejilla idéntica sobre el documento.
6. Las letras ocultas quedaban visibles a través de las ventanas.

Era especialmente útil porque permitía ocultar el mensaje dentro de una carta aparentemente inocente.

17. ¿Qué es la esteganografía?

La esteganografía es la ocultación de la existencia de un mensaje, no solamente de su contenido.

En un cifrado normal se sabe que existe un mensaje oculto, aunque no se conozca su significado. En la esteganografía, se intenta que el adversario ni siquiera sospeche que se está enviando una comunicación secreta.

Ejemplos históricos:

- Tinta invisible.
- Mensajes ocultos dentro de cartas normales.
- Escritura entre líneas.
- Uso de rejillas.
- Mensajes dentro de objetos cotidianos.
- Escritura en dientes huecos o prendas de vestir.

18. ¿Qué es el sistema de Porta?

El sistema de Giovanni Battista della Porta utilizaba tablas y alfabetos relacionados con una clave.

La clave indicaba qué alfabeto debía utilizarse para sustituir cada letra. El sistema constituía una mejora respecto a las sustituciones simples porque no aplicaba necesariamente la misma sustitución durante todo el mensaje.

Su importancia histórica reside en que ayudó a desarrollar los sistemas polialfabéticos, en los que una misma letra del mensaje puede convertirse en letras distintas dependiendo de la posición o de la clave utilizada.

19. ¿En qué consiste el cifrado de Vigenère?

El cifrado de Vigenère es un sistema de sustitución polialfabética que utiliza una palabra clave repetida sobre el mensaje.

Por ejemplo:

```
text
Clave:   SAFE SAFE SAFE
Mensaje: MONEY NEEDED
```

Cada letra del mensaje se combina con la letra correspondiente de la clave mediante una tabla de alfabetos desplazados.

Su ventaja frente al cifrado de César es que una misma letra del mensaje no tiene necesariamente siempre la misma representación. El resultado depende de la letra de la clave que se encuentre sobre ella.

20. ¿Qué función cumple la clave en Vigenère?

La clave determina qué alfabeto se utiliza para cada posición del mensaje.

Si se emplea la clave `SAFE`, esta se repite tantas veces como sea necesario:

```
text
SAFE SAFE SAFE SAFE
```

Cada letra de la clave produce un desplazamiento diferente. Por eso, una `E` del mensaje puede cifrarse de una manera en una posición y de otra manera en una posición distinta.

La clave permite cifrar y descifrar el mensaje de forma ordenada, pero si se repite periódicamente también deja una huella que puede ser analizada.

21. ¿Por qué se consideró difícil el cifrado de Vigenère?

Durante mucho tiempo se consideró difícil porque:

- Utiliza varios alfabetos.
- Una misma letra puede representarse mediante diferentes símbolos.
- El análisis de frecuencias simple pierde eficacia.
- La clave puede tener distintas longitudes.
- El texto cifrado parece más irregular que una sustitución monoalfabética.

Sin embargo, no es indestructible. Si la clave es corta y se repite, pueden aparecer patrones periódicos. Esos patrones permiten intentar descubrir la longitud de la clave y dividir el criptograma en grupos analizables.

22. ¿Qué aportó Kasiski al criptoanálisis?

El mayor aporte de Friedrich Wilhelm Kasiski fue mostrar cómo atacar el cifrado de Vigenère.

Su método se basaba en dos observaciones:

1. En los idiomas naturales se repiten con frecuencia determinados grupos de letras.
2. En un mensaje suficientemente largo se repiten palabras o fragmentos.

Si grupos idénticos del criptograma aparecen separados por distancias parecidas, esas distancias pueden sugerir la longitud de la clave repetida.

Una vez estimada la longitud de la clave, el analista puede separar el mensaje en varias columnas y estudiar cada una como si fuera una sustitución simple.

23. ¿Qué es el cifrado Pigpen?

El cifrado Pigpen es una sustitución simbólica en la que las letras se representan mediante fragmentos de rejillas, líneas y puntos.

Cada símbolo corresponde a una posición dentro de una estructura geométrica. El receptor necesita conocer la tabla para convertir los símbolos en letras.

Fue utilizado por sociedades secretas y también por prisioneros durante la Guerra Civil estadounidense.

Su debilidad principal es que, si se consigue la tabla de equivalencias, el sistema puede descifrarse con facilidad.

24. ¿Qué era el cifrado baconiano?

El cifrado de Francis Bacon utilizaba dos tipos diferentes de letras o caracteres, tradicionalmente representados como a y b.

Mediante grupos de cinco elementos se podían representar las letras del alfabeto:

```
text  
aaaaa, aaaab, aaaba, aaabb...
```

La particularidad del sistema es que el mensaje podía ocultarse dentro de un texto aparentemente normal utilizando dos estilos tipográficos diferentes.

Por ejemplo, una tipografía podía representar a y otra tipografía podía representar b.

25. ¿Qué es un acróstico?

Un acróstico es un texto en el que ciertas letras situadas en posiciones especiales forman otro mensaje.

Pueden utilizarse:

- Las primeras letras de cada línea.
- Las últimas letras.
- Las segundas letras.
- Las letras de palabras seleccionadas.

Por ejemplo:

```
text  
Brilla la luna  
Cae la noche  
Oscurece el camino
```

Las primeras letras forman BCO.

Los acrósticos son una forma de ocultación de información y no necesariamente un cifrado convencional.

26. ¿Qué importancia tuvo el caso de María, reina de Escocia?

María, reina de Escocia, utilizó comunicaciones cifradas durante las conspiraciones contra Isabel I de Inglaterra.

Francis Walsingham, secretario de Estado de Isabel, creó una red de inteligencia y utilizó agentes para interceptar los mensajes de María y sus partidarios.

Uno de los agentes, Gilbert Gifford, logró copiar mensajes cifrados dirigidos a los conspiradores. Walsingham consiguió encontrar la clave y utilizar las comunicaciones como prueba contra María y otros participantes.

El caso muestra que un cifrado mal protegido puede comprometer:

- Al emisor.
- Al receptor.
- La red de agentes.
- El contenido de las conspiraciones.
- La seguridad de todo un Estado.

27. ¿Qué le ocurrió al cifrado español de más de quinientos signos?

Durante el reinado de Felipe II, los agentes españoles utilizaban un sistema con más de quinientos signos.

Los franceses capturaron algunos mensajes y se los entregaron a François Viète, matemático y experto en cifrados. Viète logró romper el sistema y durante aproximadamente dos años los franceses pudieron conocer los movimientos españoles.

Este episodio demuestra que la complejidad aparente de un sistema no garantiza su seguridad. Un cifrado con muchos símbolos puede ser vulnerable si contiene regularidades o si se reutiliza demasiado.

28. ¿Qué fue el Gran Cifrado de Luis XIV?

El Gran Cifrado de Luis XIV fue un sistema criptográfico creado por Antoine Rossignol y utilizado por Francia.

Permaneció sin descifrar durante más de dos siglos. La pérdida de la clave dificultó enormemente su interpretación.

En 1893, el comandante Bazeries consiguió resolverlo después de varios años de trabajo. Gracias a ello se identificó al llamado “hombre de la máscara de hierro” como Vivian de Bulonde, un general francés castigado por desobedecer órdenes militares.

El episodio demuestra la importancia de:

- Conservar las claves.
- Analizar documentos antiguos.
- Comparar nombres y acontecimientos históricos.
- Combinar conocimiento lingüístico, histórico y criptográfico.

29. ¿Qué era el libro de códigos?

Un libro de códigos era un diccionario en el que determinadas palabras, frases o conceptos se asociaban a números o expresiones codificadas.

Por ejemplo, un código podía asignar un número a cada sílaba inglesa o a determinadas órdenes militares.

Los libros de códigos eran eficaces porque permitían transmitir rápidamente frases conocidas. Sin embargo, tenían varios riesgos:

- Podían ser robados.
- Podían ser fotografiados o copiados.
- Su transporte resultaba peligroso.
- Era difícil sustituirlos con rapidez.
- Si el enemigo obtenía un ejemplar, podía interpretar muchos mensajes.

30. ¿Qué es un libro-código basado en un libro común?

Es un sistema en el que emisor y receptor utilizan la misma edición de un libro.

El mensaje se transmite mediante números que indican:

- Página.
- Línea.
- Palabra.
- A veces, posición de la letra.

El destinatario busca esas referencias en su ejemplar y reconstruye el mensaje.

El sistema puede parecer seguro, pero si el adversario descubre qué libro y qué edición se utilizan, puede descifrar los mensajes. Por eso, disponer del mismo libro constituye una debilidad importante.

31. ¿Por qué Morse no es estrictamente un código?

Morse representa las letras mediante combinaciones de puntos y rayas.

No sustituye necesariamente una frase completa por una palabra o número, sino que representa cada letra individualmente. Por esa razón, desde el punto de vista técnico, es un sistema de representación o cifrado, aunque tradicionalmente se conozca como “código Morse”.

Su gran ventaja es que puede transmitirse mediante:

- Corriente eléctrica.
- Luces.
- Silbidos.
- Banderas.
- Golpes o sonidos.

Samuel Morse asignó símbolos breves a las letras de mayor frecuencia. Por ejemplo, la E se representa con un solo punto.

32. ¿Qué problema sufrió el ejército turco con su sistema cifrado?

El mariscal otomano Osman Pasha confió el código a Selim Pasha, que era el jefe de cifrado.

Selim llevó consigo el código cuando salió de misión. Como nadie más conocía el sistema y nadie consiguió romperlo, los telegramas cifrados se acumularon sin poder ser leídos.

El problema no fue únicamente técnico, sino organizativo:

- Se concentró el conocimiento en una sola persona.
- No existía una copia de seguridad operativa.
- El sistema dependía completamente de un individuo.
- La ausencia del responsable paralizó las comunicaciones.

33. ¿Qué es el cifrado de Saint-Cyr?

El cifrado de Saint-Cyr utiliza alfabetos colocados en tiras o placas deslizantes.

Una fila permanece fija y otra puede moverse. La clave determina la posición de los alfabetos. Una vez colocados, se busca la correspondencia entre las letras del mensaje y las letras cifradas.

Es más rápido que algunos sistemas manuales y permite modificar la sustitución mediante la posición de la tira.

34. ¿Qué es el cifrado Playfair?

El cifrado Playfair es un sistema de sustitución que cifra las letras por parejas.

Se construye una cuadrícula de letras, normalmente de cinco por cinco, combinando I y J o eliminando una de ellas. La palabra clave determina la colocación inicial de las letras.

Las parejas de letras se transforman siguiendo reglas basadas en su posición dentro de la cuadrícula:

- Si están en la misma fila, se sustituyen por las letras situadas a la derecha.
- Si están en la misma columna, se sustituyen por las letras situadas debajo.
- Si forman un rectángulo, cada letra adopta la columna de la otra.

Al operar con pares, el análisis de frecuencias de letras individuales resulta menos directo.

35. ¿Qué es una transmisión clandestina?

Es el envío secreto de información evitando que el adversario descubra el mensaje o la identidad del comunicante.

No basta con cifrar el contenido. También hay que proteger:

- La existencia de la comunicación.
- La identidad del emisor.
- La identidad del receptor.
- El medio de transmisión.

- La fecha y el lugar.
- La clave utilizada.

Los espías podían emplear cartas, tinta invisible, mensajes ocultos en objetos, entregas indirectas o sistemas de señales.

36. ¿Qué es la tinta invisible?

La tinta invisible permite escribir un mensaje que no se observa a simple vista. El texto aparece después de aplicar calor, sustancias químicas u otro procedimiento.

Su ventaja es que la carta puede parecer ordinaria. Su debilidad es que el adversario puede sospechar de una comunicación aparentemente extraña o analizar el papel.

La tinta invisible es principalmente un recurso de esteganografía, porque intenta ocultar que existe un mensaje.

37. ¿Qué problemas presenta una comunicación secreta?

Una comunicación secreta puede fallar por varias razones:

- La clave puede ser robada.
- El mensaje puede ser interceptado.
- El receptor puede perder la clave.
- El texto puede contener errores.
- El método puede repetirse demasiado.
- El adversario puede reconocer el patrón.
- El emisor puede revelar información sobre sí mismo.
- El medio de transmisión puede resultar sospechoso.
- El mensaje puede ser demasiado largo.
- La organización puede depender de una única persona.

Por tanto, la seguridad no depende solamente del cifrado. También depende del procedimiento completo.

38. ¿Qué importancia tiene un error en un cifrado?

Un error puede provocar que el destinatario no pueda interpretar el mensaje o lo interprete de manera equivocada.

En ciertos casos, un error puede tener consecuencias políticas o militares graves. La obra relata el caso de Federico de Brandeburgo, que recibió un mensaje ambiguo en el que no sabía si debía dirigirse a la persona número 110 o a la número 116.

Por impaciencia, escribió a la persona equivocada, el padre Wolf. El error terminó favoreciendo sus intereses y contribuyó a que Prusia se convirtiera en reino.

Este caso muestra que un error puede:

- Destruir una operación.
- Provocar una decisión equivocada.
- Retrasar una respuesta.
- Ocasionalmente, producir un resultado inesperadamente favorable.

39. ¿Qué es la frecuencia de letras?

La frecuencia de letras es el número de veces que aparece cada letra en un texto.

En un idioma determinado, algunas letras aparecen más veces que otras. En inglés, la E es normalmente una de las más frecuentes. En español, suelen ser frecuentes letras como E, A, O, S y N.

En una sustitución monoalfabética, las frecuencias del mensaje original suelen conservarse parcialmente, aunque las letras hayan cambiado de símbolo.

Por ejemplo, si un símbolo aparece mucho más que los demás, podría representar una letra frecuente del idioma.

40. ¿Qué son los bigramas?

Los bigramas son grupos de dos letras.

Ejemplos:

- TH en inglés.
- HE en inglés.
- DE en español.
- ES en español.
- EN en español.

Los bigramas ayudan a reconocer un idioma y a formular hipótesis sobre un criptograma. Si una pareja de símbolos aparece muchas veces, puede corresponder a una pareja frecuente del idioma.

41. ¿Qué son los trigramas?

Los trigramas son grupos de tres letras.

Ejemplos:

- THE en inglés.
- ING en inglés.
- QUE en español.
- EST en español.

- LOS en español.

El análisis de trigramas puede ser más informativo que el análisis de letras aisladas porque proporciona unidades lingüísticas mayores.

42. ¿Qué importancia tienen las letras dobles?

Las letras dobles son repeticiones consecutivas de una misma letra, como:

- LL.
- RR.
- SS.
- EE.
- OO.

En un criptograma, una pareja de símbolos idénticos puede indicar una letra doble. No constituye una prueba definitiva, pero sirve para formular hipótesis.

El analista debe estudiar si la repetición aparece:

- Al principio de una palabra.
- En el centro.
- Al final.
- En varias palabras con estructuras semejantes.

43. ¿Cómo se puede atacar una sustitución simple?

Un procedimiento básico sería:

1. Separar las palabras, si el criptograma conserva los espacios.
2. Contar la frecuencia de cada símbolo.
3. Comparar las frecuencias con las del idioma.
4. Buscar palabras de una sola letra.
5. Analizar bigramas y trigramas.
6. Buscar letras dobles.
7. Formular una primera hipótesis de sustitución.
8. Comprobar si produce palabras coherentes.
9. Revisar las hipótesis que generen contradicciones.
10. Completar gradualmente el alfabeto de sustitución.

No conviene aceptar una hipótesis solo porque explica una palabra. Debe explicar muchas palabras y mantener una estructura lingüística coherente.

44. ¿Cómo se resolvió el mensaje de de Rohan?

El mensaje cifrado era:

MG EULHXCCLGU GHJ YXUJ LM CT ULGC ALJ

El análisis de las frecuencias mostró que algunos símbolos aparecían varias veces. El analista supuso que una de las letras más repetidas podía representar la E, una letra frecuente en francés.

A partir de esa hipótesis se fueron identificando palabras cortas y frecuentes. Finalmente, el mensaje se reconstruyó como:

LE PRISONNIER EST MORT; IL N'A RIEN DIT.

En español:

El prisionero está muerto; no dijo nada.

El caso demuestra que el análisis de frecuencias puede ser decisivo para romper una sustitución simple.

45. ¿Qué es el criptoanálisis?

El criptoanálisis es el estudio de los métodos utilizados para analizar y descifrar mensajes protegidos sin disponer necesariamente de la clave.

El criptoanalista intenta descubrir:

- El tipo de sistema.
- La clave.
- La estructura del mensaje.
- Las regularidades del idioma.
- Los errores del emisor.
- Las repeticiones.
- Las debilidades del método.

El criptoanálisis no consiste en adivinar al azar. Es un proceso de observación, formulación de hipótesis, comprobación y corrección.

46. ¿Qué debe preguntarse un analista ante un mensaje desconocido?

Debe seguir una serie de preguntas ordenadas:

1. ¿Estoy ante un mensaje real o ante un texto sin significado?
2. ¿Se trata de un código, un cifrado o una ocultación?
3. ¿Se conservan los espacios entre palabras?
4. ¿Qué símbolos aparecen y con qué frecuencia?
5. ¿Existen repeticiones?

6. ¿Hay letras dobles?
7. ¿Hay bigramas o trigramas repetidos?
8. ¿Las letras parecen sustituidas?
9. ¿Las letras originales parecen reorganizadas?
10. ¿Podría tratarse de una transposición?
11. ¿Hay una clave visible?
12. ¿Se repite una palabra clave?
13. ¿El mensaje contiene nulos?
14. ¿Qué hipótesis explica más características?
15. ¿Cómo puedo comprobarla?

47. ¿Qué huellas deja una sustitución?

Una sustitución puede dejar las siguientes huellas:

- Frecuencias desiguales.
- Repetición de símbolos en posiciones equivalentes.
- Palabras con patrones repetidos.
- Letras dobles.
- Longitudes de palabras similares al idioma original.
- Un mismo símbolo que representa siempre la misma letra en una sustitución simple.

Por ejemplo, si una palabra cifrada tiene el patrón ABBCD, podría corresponder a una palabra cuyo patrón sea:

- Primera letra diferente.
- Segunda y tercera letras iguales.
- Cuarta y quinta letras diferentes.

La forma de la palabra puede sobrevivir aunque las letras hayan sido sustituidas.

48. ¿Qué huellas deja una transposición?

Una transposición puede dejar:

- Las mismas frecuencias de letras que el texto original.
- Las mismas letras, pero en un orden extraño.
- Fragmentos de palabras rotos.
- Secuencias que parecen casi lingüísticas.
- Una longitud total idéntica a la del mensaje original.

- Posibles patrones geométricos o columnas.

Si las frecuencias parecen propias del idioma, pero el texto no forma palabras, conviene considerar la posibilidad de una transposición.

49. ¿Qué debilidades tienen los códigos?

Los códigos presentan varias debilidades:

- El libro de códigos puede ser capturado.
- El vocabulario es limitado.
- Puede resultar necesario cambiar todo el sistema si se compromete.
- Los mensajes pueden revelar qué conceptos son importantes.
- Una misma palabra codificada puede tener siempre el mismo significado.
- El código puede resultar vulnerable al análisis de mensajes repetidos.

Su ventaja es que permiten transmitir rápidamente frases habituales y pueden ocultar el contenido de manera eficiente.

50. ¿Qué debilidades tienen los cifrados simples?

Los cifrados simples suelen ser vulnerables porque:

- Mantienen patrones lingüísticos.
- Reutilizan la misma sustitución.
- Conservan frecuencias.
- Tienen pocas claves.
- Pueden romperse con suficiente texto.
- No protegen necesariamente la existencia del mensaje.
- Los errores del operador pueden revelar información.

La seguridad depende tanto del método como de su correcta utilización.

51. ¿Por qué los ejércitos y los diplomáticos utilizaban sistemas distintos?

Los ejércitos necesitaban comunicarse en condiciones móviles y peligrosas. Transportar grandes libros de códigos podía ser arriesgado, por lo que utilizaban con frecuencia cifrados.

Los barcos de guerra, en cambio, podían conservar libros de códigos protegidos. Incluso podían lastrarlos para hundirlos si existía peligro de captura.

Los diplomáticos utilizaban códigos y cifrados. Preferían los cifrados cuando necesitaban expresar matices y mensajes complejos.

Los agentes secretos podían preferir códigos o técnicas de ocultación, porque un mensaje corto o invisible era menos sospechoso.

52. ¿Qué es la arquitectura del secreto?

La arquitectura del secreto es la relación completa entre todas las fases de una comunicación protegida:

Mensaje → Código o cifrado → Clave → Transmisión → Interceptación → Análisis → Descifrado

No se debe estudiar únicamente el método que convierte el mensaje en un criptograma. También hay que analizar:

- Cómo se prepara el mensaje.
- Cómo se distribuye la clave.
- Qué canal se utiliza.
- Quién puede interceptarlo.
- Qué errores pueden producirse.
- Qué huellas quedan.
- Cómo podría atacarlo un adversario.

53. ¿Por qué no basta con conocer el nombre de un cifrado?

Conocer que un mensaje utiliza César, Vigenère, Playfair o una transposición no significa que el mensaje ya esté resuelto.

Es necesario comprender:

- Qué operación realiza el sistema.
- Qué clave utiliza.
- Cómo se aplica la clave.
- Qué estructura conserva.
- Qué huellas deja.
- Qué debilidades puede aprovechar el analista.

Por ejemplo, identificar un mensaje como Vigenère es solo el primer paso. Después hay que intentar descubrir la longitud y el contenido de la clave.

54. ¿Cuál es la importancia histórica de los códigos y cifrados?

Los códigos y cifrados influyeron en guerras, conspiraciones, diplomacia, espionaje y decisiones políticas.

Un mensaje cifrado podía:

- Alertar sobre una invasión.
- Revelar una conspiración.
- Provocar la caída de un gobernante.

- Salvar la vida de un prisionero.
- Permitir la victoria en una batalla.
- Evitar una guerra.
- Exponer los movimientos de un ejército.

La historia de la criptografía es también la historia de la lucha entre quienes desean proteger una comunicación y quienes intentan descubrirla.

55. Explica el caso de los mensajes del desembarco de Normandía

Antes del desembarco de Normandía, la BBC transmitió mensajes aparentemente absurdos dirigidos a la Resistencia francesa.

Una primera frase fue:

“Los largos sollozos de los violines del otoño.”

La segunda parte fue:

“Hieren mi corazón con una languidez monótona.”

Estas frases, tomadas de un poema de Verlaine, servían como señales acordadas. La primera advertía de que la invasión se aproximaba. La segunda indicaba que comenzaría dentro de un plazo muy breve.

Otros mensajes, como “Hace calor en Suez” o “Los dados están sobre la mesa”, ordenaban acciones concretas de sabotaje.

Este ejemplo muestra que un código puede ocultar un mensaje completo detrás de una frase aparentemente normal.

56. ¿Qué diferencia existe entre descifrar y decodificar?

Decodificar significa convertir un mensaje escrito mediante un código en el significado correspondiente, utilizando el código o diccionario adecuado.

Descifrar significa recuperar el mensaje original a partir de un cifrado, normalmente aplicando la clave o descubriendo el procedimiento.

En la práctica, ambos términos se utilizan a veces de forma general, pero la distinción técnica es importante para el examen.

57. ¿Qué significa que un sistema sea polialfabético?

Significa que utiliza varios alfabetos de sustitución en lugar de uno solo.

En una sustitución monoalfabética, una letra del mensaje siempre se transforma en el mismo símbolo.

En una sustitución polialfabética, la transformación cambia según:

- La posición de la letra.

- La letra de la clave.
- El alfabeto seleccionado.
- El ciclo de repetición.

Vigenère es el ejemplo principal estudiado en la obra.

58. ¿Qué son los nulos?

Los nulos son letras o símbolos añadidos a un mensaje sin significado propio.

Pueden utilizarse para:

- Completar grupos de longitud fija.
- Ocultar la longitud real del mensaje.
- Disimular la estructura.
- Evitar que queden espacios o posiciones vacías.

Sin embargo, si se utilizan siempre letras muy llamativas, como X o Z, el adversario puede reconocerlas. Por eso conviene que los nulos parezcan letras normales.

59. ¿Qué es una cámara negra?

Una cámara negra era una oficina secreta dedicada a interceptar, abrir, copiar y volver a cerrar correspondencia.

El ejemplo de Dresde muestra cómo las autoridades podían interceptar cartas durante el cambio de caballos de las diligencias. Los documentos se enviaban a la cámara negra, donde eran examinados y después devueltos al correo antes de que los destinatarios advirtieran la manipulación.

La operación no dependía únicamente del criptoanálisis. También exigía:

- Acceso físico al correo.
- Rapidez.
- Personal especializado.
- Discreción.
- Capacidad para volver a sellar los documentos.

60. ¿Qué respuesta completa darías a la pregunta: “¿Cómo se analiza un criptograma?”

Primero se observa el mensaje sin intentar adivinar inmediatamente su contenido. Se estudian los símbolos, los espacios, la longitud, las repeticiones y las frecuencias.

Después se determina si probablemente se trata de un código, una sustitución, una transposición o una combinación. Si las letras parecen ser las mismas que las del idioma, pero están desordenadas, se considera una transposición. Si se han reemplazado por otros símbolos, se analiza una posible sustitución.

A continuación se estudian letras frecuentes, palabras cortas, letras dobles, bigramas y trigramas. Se formulan hipótesis sobre determinadas equivalencias y se comprueba si permiten reconstruir palabras y frases coherentes.

Finalmente, se revisan las hipótesis, se corrigen las contradicciones y se intenta explicar todo el mensaje, no solo una parte.

61. Pregunta de desarrollo: explica la arquitectura del secreto

La arquitectura del secreto comienza con un mensaje que el emisor desea proteger. Ese mensaje se transforma mediante un código o un cifrado, utilizando una clave o un procedimiento previamente acordado.

Después debe transmitirse por un canal que puede ser interceptado. El adversario puede obtener el criptograma, analizar sus características, identificar regularidades y formular hipótesis sobre el método o la clave.

El proceso termina cuando el destinatario legítimo descifra el mensaje o cuando el adversario logra romperlo. Por ello, la seguridad depende de todas las etapas y no solo de la transformación criptográfica.

62. Pregunta de desarrollo: compara sustitución y transposición

La sustitución cambia los símbolos que representan el mensaje. La transposición conserva los símbolos originales, pero altera su orden.

La sustitución puede dejar huellas estadísticas porque una letra del mensaje se transforma repetidamente en el mismo símbolo. La transposición conserva las frecuencias de las letras, pero destruye las palabras y puede crear secuencias desordenadas.

Ambos sistemas pueden combinarse. En general, la combinación es más compleja, pero también puede presentar patrones si se utiliza de forma repetitiva o sin suficiente variación.

63. Pregunta de desarrollo: explica cómo se rompe una sustitución simple

Para romper una sustitución simple se comienza contando la frecuencia de los símbolos. Se compara esa distribución con la frecuencia habitual de las letras del idioma.

Después se buscan palabras cortas, letras dobles y secuencias frecuentes. Una hipótesis inicial puede asignar el símbolo más frecuente a una letra frecuente, pero debe comprobarse en todo el mensaje.

El analista construye gradualmente una tabla de equivalencias. Cada propuesta debe generar palabras y frases coherentes. Si una hipótesis produce contradicciones, se modifica o se abandona.

64. Pregunta de desarrollo: explica por qué Vigenère es más fuerte que César

César utiliza un único alfabeto y aplica siempre el mismo desplazamiento. Vigenère utiliza varios alfabetos controlados por una palabra clave.

Como consecuencia, una misma letra del mensaje puede transformarse en diferentes símbolos. Esto dificulta el análisis de frecuencia simple.

Sin embargo, si la clave de Vigenère es corta y se repite, el criptograma puede presentar periodicidad. El método de Kasiski utiliza las repeticiones para estimar la longitud de la clave y después analizar cada posición por separado.

65. Pregunta de desarrollo: ¿qué puede aprender un analista de una comunicación interceptada?

Puede obtener información sobre el contenido, pero también sobre la estructura del sistema:

- Longitud del mensaje.
- Frecuencia de los símbolos.
- Número de palabras.
- Repetición de expresiones.
- Posible idioma.
- Tipo de cifrado.
- Existencia de una clave.
- Longitud probable de la clave.
- Hábitos del emisor.
- Errores de transmisión.
- Identidad o función de los comunicantes.

Por eso, incluso un mensaje que no ha sido descifrado completamente puede proporcionar inteligencia útil.

66. Pregunta final: explica la frase “No basta con observar el mensaje; hay que comprender su estructura”

La frase significa que el analista no debe limitarse a mirar el contenido superficial del criptograma. Debe estudiar cómo está construido.

Debe observar la forma de las palabras, la repetición de símbolos, la distribución de frecuencias, la longitud de los grupos, la existencia de letras dobles y la posible presencia de una clave.

Cada sistema deja una huella. La sustitución, la transposición, los códigos y los métodos esteganográficos producen señales diferentes. Comprender esas señales permite formular hipótesis y comprobarlas.

Por tanto, descifrar no consiste solo en leer un texto oculto, sino en reconstruir el procedimiento que lo generó.