THE BRIDGE

CYBER SECURITY

# Criptografía

# Criptografía

- De forma simplificada se puede considerar que **la criptografía** es una ciencia que se encarga de desarrollar algoritmos con el  proteger la información.

- **Seguridad informática** protege las instalaciones informáticas y la información de medios digitales mientras que **la seguridad de la información** protege la información independientemente del medio en el que se encuentre.

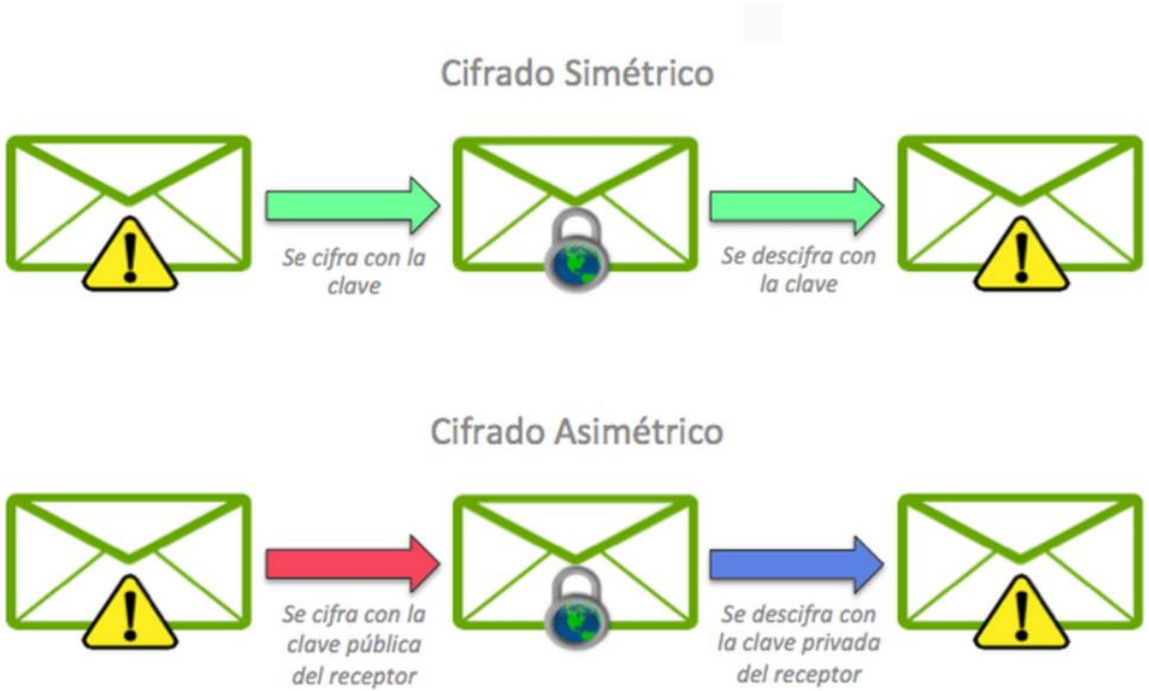
- El pilar fundamental de la seguridad de la información es **la triada CIA:**
  - **Confidencialidad** - protección de la información de los accesos no autorizados
  - **Integridad** - garantiza que la información es fiable y precisa, es decir no ha sido modificada de forma ilícita.
  - **Disponibilidad** - garantía de acceso confiable a la información por parte de las personas autorizadas, es decir debe estar accesible.

- En la seguridad de la información hay que tener en cuenta también los conceptos de **autenticación, control de acceso, no repudio y trazabilidad**.

- Conceptos de criptografía:
  - **Estenografía**: disciplina para ocultar mensajes.
  - **Cifrar**: proceso que transforman un mensaje mediante un algoritmo y una o varias claves.
  - **Codificar**: conversión de datos a otro formato con una equivalencia fija (ej. codificar en morse)

# Criptografía

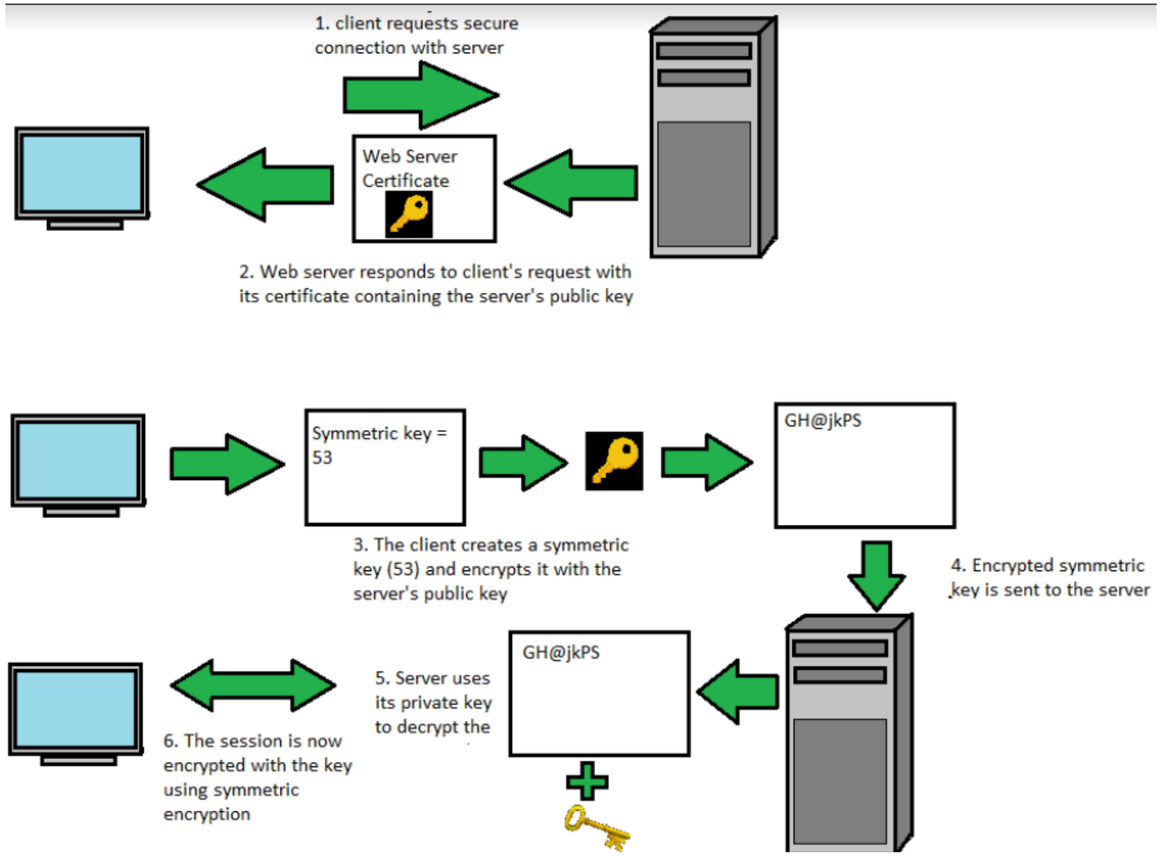
- Tipos de cifra:
  - **Cifra clásica**: ej cifrado del César ROT13
  - **Cifra moderna**
    - Según el tipo de clave:
      - **Criptografía de clave simétrica:** La criptografía simétrica solo utiliza una clave para cifrar y descifrar el mensaje, que tiene que conocer el emisor y el receptor previamente.
        - Algoritmo típico: AES
      - **Criptografía de clave asimétrica:** La criptografía asimétrica se basa en el uso de dos claves diferentes en cada uno de los extremos de la comunicación, una para cifrar y otra para descifrar: la **pública** (que se puede difundir a todas las personas que necesiten comunicarse) y la **privada** (que no debe de ser revelada nunca). Las claves privada-pública se generan simultáneamente y están ligadas una a la otra. Con una de ellas se cifra y con la otra de descifra.
        - Algoritmos típicos: RSA, DSA, Diffie-Hellman




https://forum.huawei.com/enterprise/es/capa-fisica/thread/667239755022221312-667212881550258176

# Criptografía

- Comparativa clave simétrica y clave asimétrica
  - La criptografía simétrica es rápida y eficiente para el cifrado de grandes cantidades de datos, pero es vulnerable si la clave secreta se divulga.
  - La criptografía asimétrica es más segura ya que utiliza un par de claves diferentes, pero es más lenta y menos eficiente que el cifrado simétrico.
  - Ambos tipos de cifrado se utilizan ampliamente en diferentes escenarios para garantizar la seguridad y privacidad de la información.
  - Es habitual usar **criptografía híbrida**, que es la unión de la criptología simétrica y asimétrica, como por ejemplo en el **handshake de una conexión https**:
    - Se usa cifrado asimétrico para intercambiar la clave simétrica de un solo uso para dicha sesión https, una vez hecho el intercambio de la clave simétrica de forma segura, a partir de ese momento la comunicación se realiza con dicha clave de manera rápida y segura.
    - Por cada nueva sesión se realiza de nuevo el proceso generando cada vez una clave simétrica diferente.




https://thecybersecurityman.com/2017/11/22/how-does-https-work/?authuser=0

# Criptografía

- Tipos de **codificación** básicos:
  - **ASCII**: código ASCII original tenía sólo 7 bits y el octavo bit se usaba como paridad para el control de errores.
  - **ASCII extendido**: el código más utilizado es el ASCII extendido de 256 caracteres, con el que codificamos un conjunto de letras, números y símbolos mediante cadenas de 8 bits.
  - **Base64**: el problema del código ASCII es que incluye elementos imprimibles y no imprimibles lo que daba problemas de compatibilidad por lo que se creó el Base64 que es un código intermedio de 6 bits con todos sus elementos imprimibles.

## Código ASCII Extendido

| Binario | Dec | Símbolo | Binario | Dec | Símbolo | Binario | Dec | Símbolo | Binario | Dec | Símbolo | Binario | Dec | Símbolo | Binario | Dec | Símbolo | Binario | Dec | Símbolo | Binario | Dec | Símbolo |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0000 0000 | 0 | Carácter Nulo | 0010 0000 | 32 | espacio en blanco | 0100 0000 | 64 | @ | 0110 0000 | 96 | ` | 10000000 | 128 | € | 10100000 | 160 | | 11000000 | 192 | À | 11100000 | 224 | à |
| 0000 0001 | 1 | Inicio de Encabezado | 0010 0001 | 33 | ! | 0100 0001 | 65 | A | 0110 0001 | 97 | a | 10000001 | 129 | | 10100001 | 161 | ¡ | 11000001 | 193 | Á | 11100001 | 225 | á |
| 0000 0010 | 2 | Inicio de Texto | 0010 0010 | 34 | " | 0100 0010 | 66 | B | 0110 0010 | 98 | b | 10000010 | 130 | ‚ | 10100010 | 162 | ¢ | 11000010 | 194 | Â | 11100010 | 226 | â |
| 0000 0011 | 3 | Fin de Texto | 0010 0011 | 35 | # | 0100 0011 | 67 | C | 0110 0011 | 99 | c | 10000011 | 131 | ƒ | 10100011 | 163 | £ | 11000011 | 195 | Ã | 11100011 | 227 | ã |
| 0000 0100 | 4 | Fin de Transmisión | 0010 0100 | 36 | $ | 0100 0100 | 68 | D | 0110 0100 | 100 | d | 10000100 | 132 | „ | 10100100 | 164 | ¤ | 11000100 | 196 | Ä | 11100100 | 228 | ä |
| 0000 0101 | 5 | Consulta | 0010 0101 | 37 | % | 0100 0101 | 69 | E | 0110 0101 | 101 | e | 10000101 | 133 | … | 10100101 | 165 | ¥ | 11000101 | 197 | Å | 11100101 | 229 | å |
| 0000 0110 | 6 | Acuse de recibo | 0010 0110 | 38 | & | 0100 0110 | 70 | F | 0110 0110 | 102 | f | 10000110 | 134 | † | 10100110 | 166 | ¦ | 11000110 | 198 | Æ | 11100110 | 230 | æ |
| 0000 0111 | 7 | Timbre | 0010 0111 | 39 | ' | 0100 0111 | 71 | G | 0110 0111 | 103 | g | 10000111 | 135 | ‡ | 10100111 | 167 | § | 11000111 | 199 | Ç | 11100111 | 231 | ç |
| 0000 1000 | 8 | Retroceso | 0010 1000 | 40 | ( | 0100 1000 | 72 | H | 0110 1000 | 104 | h | 10001000 | 136 | ˆ | 10101000 | 168 | ¨ | 11001000 | 200 | È | 11101000 | 232 | è |
| 0000 1001 | 9 | Tabulación horizontal | 0010 1001 | 41 | ) | 0100 1001 | 73 | I | 0110 1001 | 105 | i | 10001001 | 137 | ‰ | 10101001 | 169 | © | 11001001 | 201 | É | 11101001 | 233 | é |
| 0000 1010 | 10 | Salto de línea | 0010 1010 | 42 | * | 0100 1010 | 74 | J | 0110 1010 | 106 | j | 10001010 | 138 | Š | 10101010 | 170 | ª | 11001010 | 202 | Ê | 11101010 | 234 | ê |
| 0000 1011 | 11 | Tabulación Vertical | 0010 1011 | 43 | + | 0100 1011 | 75 | K | 0110 1011 | 107 | k | 10001011 | 139 | ‹ | 10101011 | 171 | « | 11001011 | 203 | Ë | 11101011 | 235 | ë |
| 0000 1100 | 12 | Avance de página | 0010 1100 | 44 | , | 0100 1100 | 76 | L | 0110 1100 | 108 | l | 10001100 | 140 | Œ | 10101100 | 172 | ¬ | 11001100 | 204 | Ì | 11101100 | 236 | ì |
| 0000 1101 | 13 | Retorno de carro | 0010 1101 | 45 | - | 0100 1101 | 77 | M | 0110 1101 | 109 | m | 10001101 | 141 | | 10101101 | 173 | | 11001101 | 205 | Í | 11101101 | 237 | í |
| 0000 1110 | 14 | Desactivar mayúsculas | 0010 1110 | 46 | . | 0100 1110 | 78 | N | 0110 1110 | 110 | n | 10001110 | 142 | Ž | 10101110 | 174 | ® | 11001110 | 206 | Î | 11101110 | 238 | î |
| 0000 1111 | 15 | Activar mayúsculas | 0010 1111 | 47 | / | 0100 1111 | 79 | O | 0110 1111 | 111 | o | 10001111 | 143 | | 10101111 | 175 | ¯ | 11001111 | 207 | Ï | 11101111 | 239 | ï |
| 0001 0000 | 16 | Escape vínculo de datos | 0011 0000 | 48 | 0 | 0101 0000 | 80 | P | 0111 0000 | 112 | p | 10010000 | 144 | | 10110000 | 176 | ° | 11010000 | 208 | Ð | 11110000 | 240 | ð |
| 0001 0001 | 17 | Control de dispositivo 1 (XON) | 0011 0001 | 49 | 1 | 0101 0001 | 81 | Q | 0111 0001 | 113 | q | 10010001 | 145 | ‘ | 10110001 | 177 | ± | 11010001 | 209 | Ñ | 11110001 | 241 | ñ |
| 0001 0010 | 18 | Control de dispositivo 2 | 0011 0010 | 50 | 2 | 0101 0010 | 82 | R | 0111 0010 | 114 | r | 10010010 | 146 | ’ | 10110010 | 178 | ² | 11010010 | 210 | Ò | 11110010 | 242 | ò |
| 0001 0011 | 19 | Control de dispositivo 3 (XOFF) | 0011 0011 | 51 | 3 | 0101 0011 | 83 | S | 0111 0011 | 115 | s | 10010011 | 147 | “ | 10110011 | 179 | ³ | 11010011 | 211 | Ó | 11110011 | 243 | ó |
| 0001 0100 | 20 | Control de dispositivo 4 | 0011 0100 | 52 | 4 | 0101 0100 | 84 | T | 0111 0100 | 116 | t | 10010100 | 148 | ” | 10110100 | 180 | ´ | 11010100 | 212 | Ô | 11110100 | 244 | ô |
| 0001 0101 | 21 | Acuse de recibo negativo | 0011 0101 | 53 | 5 | 0101 0101 | 85 | U | 0111 0101 | 117 | u | 10010101 | 149 | • | 10110101 | 181 | µ | 11010101 | 213 | Õ | 11110101 | 245 | õ |
| 0001 0110 | 22 | Síncronía en espera | 0011 0110 | 54 | 6 | 0101 0110 | 86 | V | 0111 0110 | 118 | v | 10010110 | 150 | – | 10110110 | 182 | ¶ | 11010110 | 214 | Ö | 11110110 | 246 | ö |
| 0001 0111 | 23 | Fin del bloque de transmisión | 0011 0111 | 55 | 7 | 0101 0111 | 87 | W | 0111 0111 | 119 | w | 10010111 | 151 | — | 10110111 | 183 | · | 11010111 | 215 | × | 11110111 | 247 | ÷ |
| 0001 1000 | 24 | Cancelar | 0011 1000 | 56 | 8 | 0101 1000 | 88 | X | 0111 1000 | 120 | x | 10011000 | 152 | ˜ | 10111000 | 184 | ¸ | 11011000 | 216 | Ø | 11111000 | 248 | ø |
| 0001 1001 | 25 | Fin del medio | 0011 1001 | 57 | 9 | 0101 1001 | 89 | Y | 0111 1001 | 121 | y | 10011001 | 153 | ™ | 10111001 | 185 | ¹ | 11011001 | 217 | Ù | 11111001 | 249 | ù |
| 0001 1010 | 26 | Substitución | 0011 1010 | 58 | : | 0101 1010 | 90 | Z | 0111 1010 | 122 | z | 10011010 | 154 | š | 10111010 | 186 | º | 11011010 | 218 | Ú | 11111010 | 250 | ú |
| 0001 1011 | 27 | Escape | 0011 1011 | 59 | ; | 0101 1011 | 91 | [ | 0111 1011 | 123 | { | 10011011 | 155 | › | 10111011 | 187 | » | 11011011 | 219 | Û | 11111011 | 251 | û |
| 0001 1100 | 28 | Separador de archivo | 0011 1100 | 60 | < | 0101 1100 | 92 | \ | 0111 1100 | 124 | \| | 10011100 | 156 | œ | 10111100 | 188 | ¼ | 11011100 | 220 | Ü | 11111100 | 252 | ü |
| 0001 1101 | 29 | Separador de grupo | 0011 1101 | 61 | = | 0101 1101 | 93 | ] | 0111 1101 | 125 | } | 10011101 | 157 | | 10111101 | 189 | ½ | 11011101 | 221 | Ý | 11111101 | 253 | ý |
| 0001 1110 | 30 | Separador de registro | 0011 1110 | 62 | > | 0101 1110 | 94 | ^ | 0111 1110 | 126 | ~ | 10011110 | 158 | ž | 10111110 | 190 | ¾ | 11011110 | 222 | Þ | 11111110 | 254 | þ |
| 0001 1111 | 31 | Separador de unidad | 0011 1111 | 63 | ? | 0101 1111 | 95 | _ | 01111111 | 127 | DEL | 10011111 | 159 | Ÿ | 10111111 | 191 | ¿ | 11011111 | 223 | ß | 11111111 | 255 | ÿ |

## Código ASCII Estandar

| $b_1$ | $b_2$ | $b_3$ | $b_4$ | $b_5$ | $b_6$ | $b_7$ |
|---|---|---|---|---|---|---|

| Binario | Dec | Símbolo | Binario | Dec | Símbolo | Binario | Dec | Símbolo | Binario | Dec | Símbolo |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 0000 0000 | 0 | Carácter Nulo | 0010 0000 | 32 | espacio en blanco | 0100 0000 | 64 | @ | 0110 0000 | 96 | ` |
| 0000 0001 | 1 | Inicio de Encabezado | 0010 0001 | 33 | ! | 0100 0001 | 65 | A | 0110 0001 | 97 | a |
| 0000 0010 | 2 | Inicio de Texto | 0010 0010 | 34 | " | 0100 0010 | 66 | B | 0110 0010 | 98 | b |
| 0000 0011 | 3 | Fin de Texto | 0010 0011 | 35 | # | 0100 0011 | 67 | C | 0110 0011 | 99 | c |
| 0000 0100 | 4 | Fin de Transmisión | 0010 0100 | 36 | $ | 0100 0100 | 68 | D | 0110 0100 | 100 | d |
| 0000 0101 | 5 | Consulta | 0010 0101 | 37 | % | 0100 0101 | 69 | E | 0110 0101 | 101 | e |
| 0000 0110 | 6 | Acuse de recibo | 0010 0110 | 38 | & | 0100 0110 | 70 | F | 0110 0110 | 102 | f |
| 0000 0111 | 7 | Timbre | 0010 0111 | 39 | ' | 0100 0111 | 71 | G | 0110 0111 | 103 | g |
| 0000 1000 | 8 | Retroceso | 0010 1000 | 40 | ( | 0100 1000 | 72 | H | 0110 1000 | 104 | h |
| 0000 1001 | 9 | Tabulación horizontal | 0010 1001 | 41 | ) | 0100 1001 | 73 | I | 0110 1001 | 105 | i |
| 0000 1010 | 10 | Salto de línea | 0010 1010 | 42 | * | 0100 1010 | 74 | J | 0110 1010 | 106 | j |
| 0000 1011 | 11 | Tabulación Vertical | 0010 1011 | 43 | + | 0100 1011 | 75 | K | 0110 1011 | 107 | k |
| 0000 1100 | 12 | Avance de página | 0010 1100 | 44 | , | 0100 1100 | 76 | L | 0110 1100 | 108 | l |
| 0000 1101 | 13 | Retorno de carro | 0010 1101 | 45 | - | 0100 1101 | 77 | M | 0110 1101 | 109 | m |
| 0000 1110 | 14 | Desactivar mayúsculas | 0010 1110 | 46 | . | 0100 1110 | 78 | N | 0110 1110 | 110 | n |
| 0000 1111 | 15 | Activar mayúsculas | 0010 1111 | 47 | / | 0100 1111 | 79 | O | 0110 1111 | 111 | o |
| 0001 0000 | 16 | Escape vínculo de datos | 0011 0000 | 48 | 0 | 0101 0000 | 80 | P | 0111 0000 | 112 | p |
| 0001 0001 | 17 | Control de dispositivo 1 (XON) | 0011 0001 | 49 | 1 | 0101 0001 | 81 | Q | 0111 0001 | 113 | q |
| 0001 0010 | 18 | Control de dispositivo 2 | 0011 0010 | 50 | 2 | 0101 0010 | 82 | R | 0111 0010 | 114 | r |
| 0001 0011 | 19 | Control de dispositivo 3 (XOFF) | 0011 0011 | 51 | 3 | 0101 0011 | 83 | S | 0111 0011 | 115 | s |
| 0001 0100 | 20 | Control de dispositivo 4 | 0011 0100 | 52 | 4 | 0101 0100 | 84 | T | 0111 0100 | 116 | t |
| 0001 0101 | 21 | Acuse de recibo negativo | 0011 0101 | 53 | 5 | 0101 0101 | 85 | U | 0111 0101 | 117 | u |
| 0001 0110 | 22 | Síncronía en espera | 0011 0110 | 54 | 6 | 0101 0110 | 86 | V | 0111 0110 | 118 | v |
| 0001 0111 | 23 | Fin del bloque de transmisión | 0011 0111 | 55 | 7 | 0101 0111 | 87 | W | 0111 0111 | 119 | w |
| 0001 1000 | 24 | Cancelar | 0011 1000 | 56 | 8 | 0101 1000 | 88 | X | 0111 1000 | 120 | x |
| 0001 1001 | 25 | Fin del medio | 0011 1001 | 57 | 9 | 0101 1001 | 89 | Y | 0111 1001 | 121 | y |
| 0001 1010 | 26 | Substitución | 0011 1010 | 58 | : | 0101 1010 | 90 | Z | 0111 1010 | 122 | z |
| 0001 1011 | 27 | Escape | 0011 1011 | 59 | ; | 0101 1011 | 91 | [ | 0111 1011 | 123 | { |
| 0001 1100 | 28 | Separador de archivo | 0011 1100 | 60 | < | 0101 1100 | 92 | \ | 0111 1100 | 124 | \| |
| 0001 1101 | 29 | Separador de grupo | 0011 1101 | 61 | = | 0101 1101 | 93 | ] | 0111 1101 | 125 | } |
| 0001 1110 | 30 | Separador de registro | 0011 1110 | 62 | > | 0101 1110 | 94 | ^ | 0111 1110 | 126 | ~ |
| 0001 1111 | 31 | Separador de unidad | 0011 1111 | 63 | ? | 0101 1111 | 95 | _ | 01111111 | 127 | DEL |

## BASE 64

| VALOR | SÍMBOLO | VALOR | SÍMBOLO | VALOR | SÍMBOLO | VALOR | SÍMBOLO |
|---|---|---|---|---|---|---|---|
| 0 | A | 16 | Q | 32 | g | 48 | w |
| 1 | B | 17 | R | 33 | h | 49 | x |
| 2 | C | 18 | S | 34 | i | 50 | y |
| 3 | D | 19 | T | 35 | j | 51 | z |
| 4 | E | 20 | U | 36 | k | 52 | 0 |
| 5 | F | 21 | V | 37 | l | 53 | 1 |
| 6 | G | 22 | W | 38 | m | 54 | 2 |
| 7 | H | 23 | X | 39 | n | 55 | 3 |
| 8 | I | 24 | Y | 40 | o | 56 | 4 |
| 9 | J | 25 | Z | 41 | p | 57 | 5 |
| 10 | K | 26 | a | 42 | q | 58 | 6 |
| 11 | L | 27 | b | 43 | r | 59 | 7 |
| 12 | M | 28 | c | 44 | s | 60 | 8 |
| 13 | N | 29 | d | 45 | t | 61 | 9 |
| 14 | O | 30 | e | 46 | u | 62 | + |
| 15 | P | 31 | f | 47 | v | 63 | / |

Fuente: proyecto THOTH
https://www.youtube.com/playlist?list=PL8bSwVy8_IcNNS5QDLjV7gUg8dleMFSER&authuser=0

# Criptografía

- **Funciones HASH**

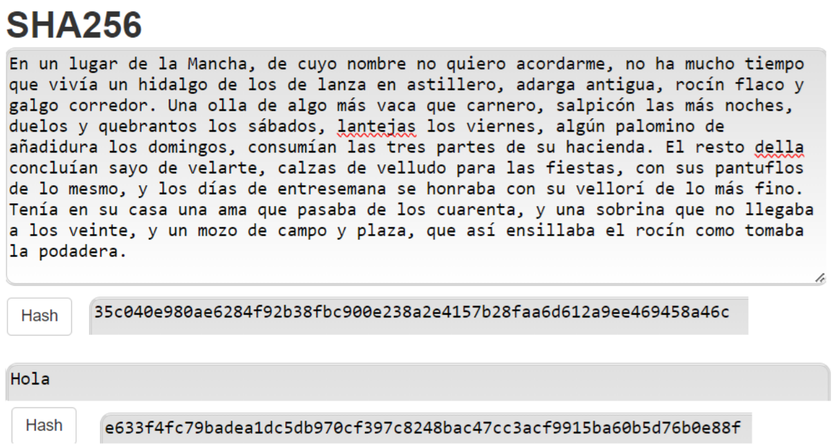
  - Una **función criptográfica hash es un algoritmo matemático** que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una **longitud fija**. Independientemente de la longitud de los datos de entrada, el valor hash de salida tendrá siempre la misma longitud dependiendo del algoritmo utilizado.

  - Se puede considerar como un identificador unívoco que muestra **la integridad de los datos**. Si aplicamos el algoritmo sobre un mismo archivo en varias ocasiones, siempre vamos a obtener la misma secuencia alfanumérica. Por el contrario, cualquier mínima alteración de los datos de entrada generarían un código hash completamente distinto.

  - Las funciones hash son **unidireccionales**. Esto quiere decir que a partir de los datos de entrada, van a generar el código hash. No obstante, partiendo del código hash, no se puede descifrar o inferir cuáles fueron los datos introducidos inicialmente.

  - Tipos de algoritmos de hash:
    - **MD5**: Se considera vulnerable. La función de hash MD5 produce un valor de hash de 128-bit.
    - **SHA-1, SHA-256, SHA-512:** SHA significa (Secure Hash Algorithm) Algoritmo de Hash Seguro.
      - SHA1 fue la primera versión del algoritmo fue SHA, genera un hash de 160-bit (20 bytes). Se considera vulnerable.
      - SHA-256 genera un hash de 32 bytes.
      - SHA-512 genera un hash de 64 bytes.

  - Usos habituales
    - Blockchain
    - Gestión de contraseñas
    - Detección de malware
    - Detección de infracciones de derechos de autor




https://emn178.github.io/online-tools/sha256.html

# Herramientas

- Herramienta web para codificar y decodificar en base64:
  - https://www.base64encode.org

- Herramientas de linux:

  - **decodify**
    - Detecta y decodifica cadenas codificadas de forma recursiva
    - https://github.com/s0md3v/Decodify

  - **hash-identifier**
    - Software para identificar los diferentes tipos de hashes utilizados
    - https://www.kali.org/tools/hash-identifier/?authuser=0

  - **checksum**
    - Un conjunto de herramientas software para generar un hash:
      - md5sum
      - sha1sum
      - sha256sum

```
└─$ sha1sum prueba.txt
5fba0d1890c13b84cd6ce9de98d9205f2a6e8eee  prueba.txt
```

```
└─$ dcode NjE0NzM5NzM1OTUxM0QzRA==
[+] Decoded from Base64 : 6147397359513D3D
[+] Decoded from Hex : aG9sYQ==
[+] Decoded from Base64 : hola
```

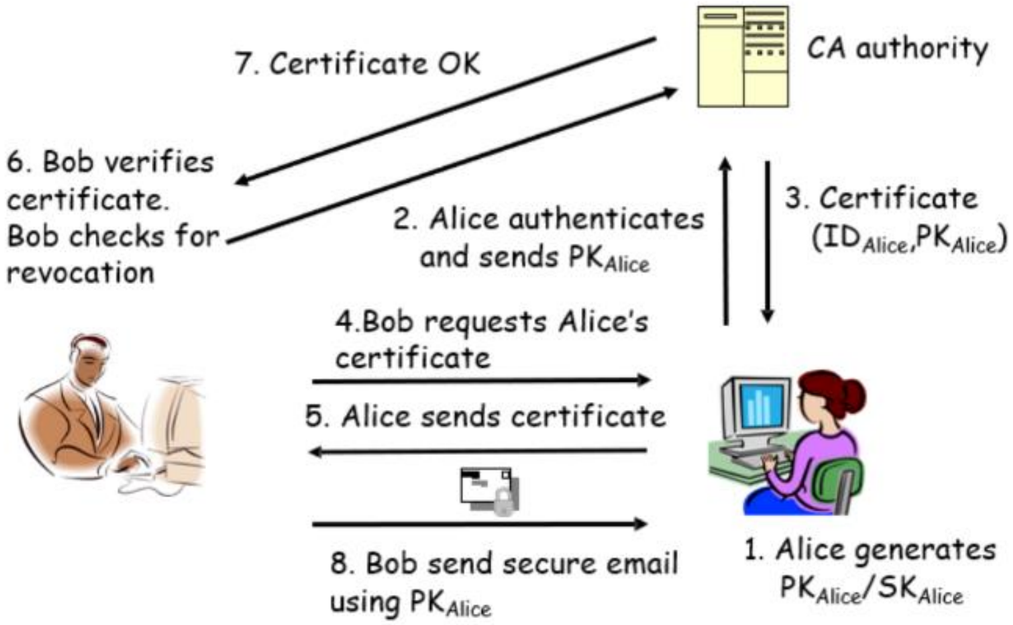
```
└─$ hash-identifier 5fba0d1890c13b84cd6ce9de98d9205f2a6e8eee
   #########################################################################
   #                                                                       #
   #                                                                       #
   #                                                                       #
   #                                                                       #
   #                                                                       #
   #                                                                       #
   #                                                                v1.2   #
   #                                                             By Zion3R #
   #                                                        www.Blackploit.com #
   #                                                        Root@Blackploit.com #
   #########################################################################
--------------------------------------------------

Possible Hashs:
[+] SHA-1
[+] MySQL5 - SHA-1(SHA-1($pass))

Least Possible Hashs:
[+] Tiger-160
[+] Haval-160
[+] RipeMD-160
[+] SHA-1(HMAC)
[+] Tiger-160(HMAC)
[+] RipeMD-160(HMAC)
```

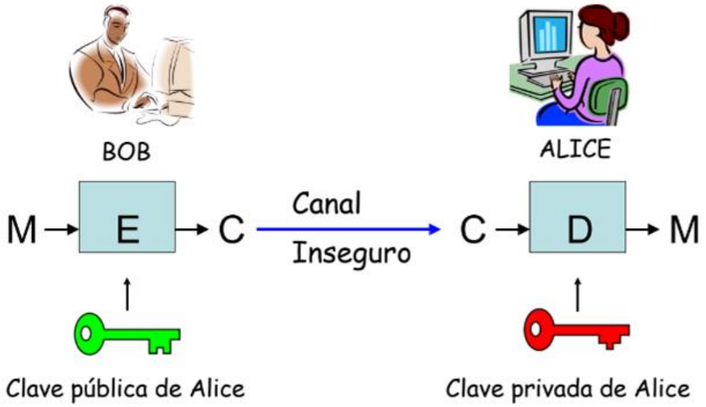
# Infraestructura de clave pública

- La infraestructura de clave pública (PKI) proporciona una forma de comprobar la identidad de un sitio remoto mediante un certificado digital. PKI utiliza una entidad de certificación (CA) para validar la información y firmarla con una firma digital de forma que ni su información ni la firma puedan modificarse. Una vez firmada, la información se convierte en un certificado digital. Los dispositivos que reciben un certificado digital pueden comprobar la información del certificado validando la firma mediante criptografía de clave pública.



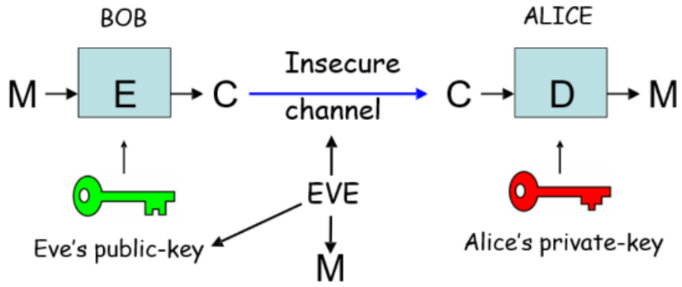
# Conceptos Infraestructura de clave pública

## Cifrado de clave pública



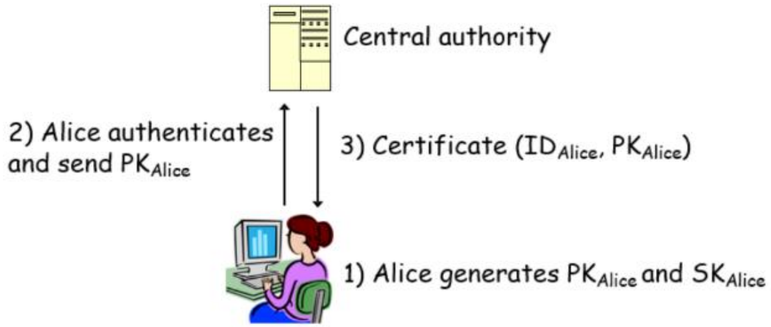

## Autenticación

- Las claves públicas deben ser autenticadas
  - Bob necesita estar seguro de que la clave pública pertenece a Alice.
  - De lo contrario, puede ocurrir un ataque de suplantación de identidad.




## Infraestructura de Clave Pública

- Una autoridad central vincula las claves públicas a las identidades.
- La clave pública se almacena en un certificado.




## Certificado de clave pública

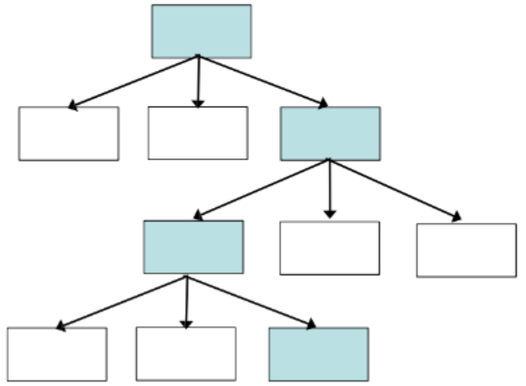
- Certificado:
  - La firma de la autoridad certificadora une una clave pública con una identidad.
  - Bob puede estar seguro de que la clave pública pertenece a Alice al verificar la firma usando la clave pública de la CA (Central Authority).
  - Todos los participantes confían en la CA.

# Conceptos Infraestructura de clave pública

- **Entidad certificadora**
  - La CA se encarga de crear certificados con la clave pública que atestiguan que la clave privada que está en el certificado se corresponde con la identidad del certificado:
  - La CA debe verificar la identidad del usuario antes de emitir el certificado.
  - Si la clave privada de la CA se ve comprometida, se pierde la seguridad.
  - Mayores proveedores de certificados: Verisign, Geotrust, Global Trusted Sign (GTS)

- **Certificado** de Clave Pública
  - Un certificado de clave pública puede incluir:
    - Clave pública del usuario.
    - Nombre (persona, equipo o empresa).
    - Período de validez.
    - Ubicación (URL) de un centro de revocación.
    - Firma digital del certificado, producida por la clave privada de la CA.
  - **Revocación** de certificado
    - Se debe revocar cuando se dan las siguientes situaciones:
      - La clave privada está comprometida.
      - La identidad y la PK (clave pública) no se corresponden.
      - Un usuario siempre debe comprobar la validez de un certificado
    - La CA puede mantener una lista de revocación de certificados (CRL)
      - Debe estar actualizada y fácilmente disponible.
    - El estandar más común de certificado es el **X509**

Jerarquía de los certificados



Ejemplo:

CA País (root certificate)

CA Comunidad Autónoma

CA Provincia

CA Municipio…

Certificado Root

- Es el que está en lo más alto de la cadena, lo más alto de la jerarquía.
- Típicamente en el estándar X509.
- Confianza implícita.
- Incluido en los navegadores web.
- Utilizado para conexiones SSL/TLS.

# SSL (Secure Sockets Layer) y TLS (Transport Layer Security)

- **Secure Sockets Layer** (capa de sockets seguros), es la tecnología estándar para mantener segura una conexión a Internet, así como para proteger cualquier información confidencial que se envía entre dos sistemas e impedir que los atacantes lean y modifiquen cualquier dato que se transfiera.

- SSL 3.0 es similar a TLS 1.0
  - Garantiza la confidencialidad, integridad y autenticidad a través de Internet (triada CIA).

- **Transport Layer Security** (seguridad de la capa de transporte) es una versión actualizada y más segura de SSL.

- Hay que confiar en el navegador que instalamos.

- Aplicaciones de SSL
  - Utilizada principalmente para asegurar HTTP -> HTTPS


THE
BRIDGE