對稱式密碼系統 作業3 F74116217 資訊甲 115 戴宇澤

需要的資料如下表所示。

|  |  |
| --- | --- |
| 明文 | "797A2E5F65656565" |
| 修改後明文 | "797A2E5F65656564" |
| 金鑰 | "696C6F7665796F75" |
| 修改後金鑰 | "696C6F7665796F74" |

1. 不同金鑰(相差1bit)加密相同明文

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Rounds | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| Differences | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

|  |  |  |
| --- | --- | --- |
| 密鑰  L[n]R[n], n= | "696C6F7665796F75" | "696C6F7665796F74" |
| 0 | 1111101100001011111111001111100100000000111101110000111100001110 | 1111101100001011111111001111100100000000111101110000111100001110 |
| 1 | 0000000011110111000011110000111010001100000001100011000101110011 | 0000000011110111000011110000111010001100000001100011000101110011 |
| 2 | 1000110000000110001100010111001100111101001000111010110000100011 | 1000110000000110001100011111001100101111000100111000100000100011 |
| 3 | 0011110100100011101011000010001101101001000100111111011010100101 | 0011110100100011101011000010001101101001000100111111011010100101 |
| 4 | 0110100100010011111101101010010101100110010111100000001110010010 | 0110100100010011111101101010010101100110010111100000001110010010 |
| 5 | 0110011001011110000000111001001011100101110010000011110000111001 | 0110011001011110000000111001001011100101110010000011110000111001 |
| 6 | 1110010111001000001111000011100110110110001110101011101101001110 | 1110010111001000001111000011100110110110001110101011101101001110 |
| 7 | 1011011000111010101110110100111001000101110000010000111011101110 | 1011011000111010101110110100111001000101110000010000111011101110 |
| 8 | 0100010111000001000011101110111001011000001101000111101101110111 | 0100010111000001000011101110111001011000001101000111101101110111 |
| 9 | 0101100000110100011110110111011111000101111100000000010000010010 | 0101100000110100011110110111011111000101111100000000010000010010 |
| 10 | 1100010111110000000001000001001000111011110100010101001011111110 | 1100010111110000000001000001001000111011110100010101001011111110 |
| 11 | 0011101111010001010100101111111010011111010001011100111011110111 | 0011101111010001010100101111111010011111010001011100111011110111 |
| 12 | 1001111101000101110011101111011101111000011000110101111101001110 | 1001111101000101110011101111011101111000011000110101111101001110 |
| 13 | 0111100001100011010111110100111000011111110000111110110101100010 | 0111100001100011010111110100111000011111110000111110110101100010 |
| 14 | 0001111111000011111011010110001000011001110011111100100100100110 | 0001111111000011111011010110001000011001110011111100100100100110 |
| 15 | 0001100111001111110010010010011001110010010010100111100110000101 | 0001100111001111110010010010011001110010010010100111100110000101 |
| 16 | 0111001001001010011110011000010101011010001111101110101110101110 | 0111001001001010011110011000010101011010001111101110101110101110 |

1. 相同金鑰加密不同明文(相差1bit)

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Rounds | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| Diff | 1 | 7 | 20 | 32 | 36 | 35 | 34 | 31 | 29 | 35 | 40 | 40 | 32 | 26 | 32 | 32 |
| % | 1.5 | 10.9 | 31.2 | 50.0 | 56.2 | 54.6 | 53.1 | 48.4 | 45.3 | 54.6 | 66.6 | 66.6 | 50.0 | 40.6 | 50.0 | 50.0 |

|  |  |  |
| --- | --- | --- |
| 明文  L[n]R[n], n= | "797A2E5F65656565" | "797A2E5F65656564" |
| 0 | 1111101100001011111111001111100100000000111101110000111100001110 | 1111101100001011111111000111100100000000111101110000111100001110 |
| 1 | 0000000011110111000011110000111010001100000001100011000101110011 | 0000000011110111000011110000111010001100000001100011000111110011 |
| 2 | 1000110000000110001100010111001100111101001000111010110000100011 | 1000110000000110001100011111001100101111000100111000100000100011 |
| 3 | 0011110100100011101011000010001101101001000100111111011010100101 | 0010111100010011100010000010001110111001001111100010010011101111 |
| 4 | 0110100100010011111101101010010101100110010111100000001110010010 | 1011100100111110001001001110111101111111110111011110010101101111 |
| 5 | 0110011001011110000000111001001011100101110010000011110000111001 | 0111111111011101111001010110111111100111001011101110101111010111 |
| 6 | 1110010111001000001111000011100110110110001110101011101101001110 | 1110011100101110111010111101011110101111100111110110100011110111 |
| 7 | 1011011000111010101110110100111001000101110000010000111011101110 | 1010111110011111011010001111011110101101000101111110001001100010 |
| 8 | 0100010111000001000011101110111001011000001101000111101101110111 | 1010110100010111111000100110001001101100010110010100100001111101 |
| 9 | 0101100000110100011110110111011111000101111100000000010000010010 | 0110110001011001010010000111110100010100001101100110000011111010 |
| 10 | 1100010111110000000001000001001000111011110100010101001011111110 | 0001010000110110011000001111101011101010011010111000111000000111 |
| 11 | 0011101111010001010100101111111010011111010001011100111011110111 | 1110101001101011100011100000011101111111101110100111101110000110 |
| 12 | 1001111101000101110011101111011101111000011000110101111101001110 | 0111111110111010011110111000011000000101111100001110011110110100 |
| 13 | 0111100001100011010111110100111000011111110000111110110101100010 | 0000010111110000111001111011010011001111100100111111100111011000 |
| 14 | 0001111111000011111011010110001000011001110011111100100100100110 | 1100111110010011111110011101100000001111110000011110011110000011 |
| 15 | 0001100111001111110010010010011001110010010010100111100110000101 | 0000111111000001111001111000001111100101100010011101111111110011 |
| 16 | 0111001001001010011110011000010101011010001111101110101110101110 | 1110010110001001110111111111001101100000000011010010100110011111 |