1)

***1.1***

***Encoded secret***:

*Message*: “This is the secret message!”

*Bytes*: [84, 104, 105, 115, 32, 105, 115, 32, 116, 104, 101, 32, 115, 101, 99, 114, 101, 116, 32, 109, 101, 115, 115, 97, 103, 101, 33]

*Binary*:

01010100

01101000

01101001

01110011

00100000

01101001

01110011

00100000

01110100

01101000

01100101

00100000

01110011

01100101

01100011

01110010

01100101

01110100

00100000

01101101

01100101

01110011

01110011

01100001

01100111

01100101

00100001

***Decoded secret***:

*Message*: “D0`/�я8�CJ��kCDi��Qz��Z”

*Bytes*: [131, 225, 72, 95, 154, 132, 248, 64, 222, 2, 157, 234, 162, 143, 61, 88, 135, 173, 123, 17, 31, 121, 244, 103, 202, 151, 159]

*Binary*:

10011001

00110011

00111101

01001101

00110110

00110111

11011011

10011111

01111011

10000111

00111000

00101011

11111110

01001111

00101010

01001101

10010110

10110101

10100001

10010001

01100110

10010000

01000101

00101000

00000010

10110100

01110011

***Longest substream***: 011010000110010

1.2 ***Longest substream***: 000000111010

1.3 ***Longest substream***: 010011001010111

1.4 ***Longest substream***: 01000110100001

1.5 ***Longest substream***: 00101011100110

1.6 ***Longest substream***: 1001010111001

1.7 ***Longest substream***: 10010000001101001

1.8 ***Longest substream***: 01000010000001

1.9 ***Longest substream***: 01101000011010

1.10 ***Longest substream***: 0101000110100

Conclusion: on average 1-2 bytes of information “survives”, however an attacker can’t predict which 1-2 bytes will survive