1) Encoded base2, sanitized base2

***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*: “F�@x��PXl��@aP"hc�”

*Bytes*: [70, 128, 64, 14, 24, 4, 120, 133, 177, 80, 4, 88, 108, 18, 136, 208, 64, 20, 97, 80, 194, 146, 34, 1, 104, 99, 184]

*Binary*:

01000110

10000000

01000000

00001110

00011000

00000100

01111000

10000101

10110001

01010000

00000100

01011000

01101100

00010010

10001000

11010000

01000000

00010100

01100001

01010000

11000010

10010010

00100010

00000001

01101000

01100011

10111000

***Longest substream***: 0110100001100

1.2 ***Longest substream***: 000010000001

1.3 ***Longest substream***: 0011011000010

1.4 ***Longest substream***: 1101000010000001

1.5 ***Longest substream***: 01000010000001

1.6 ***Longest substream***: 1001010110001

1.7 ***Longest substream***: 0000011101000

1.8 ***Longest substream***: 0010111001100

1.9 ***Longest substream***: 0100001000000

1.10 ***Longest substream***: 10100100000011

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

2) Encoded base2, sanitized base3

2.1)

***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*: “ğÀɑĻʵįŔȑɌ7,ȇǎȼǢɨōɊƦǌːȽȏ”

*Bytes*: [287, 192, 29, 593, 315, 693, 303, 340, 529, 588, 55, 44, 519, 462, 572, 482, 130, 616, 333, 14, 586, 31, 422, 460, 720, 573, 527]

*Binary*:

101122

021010

001002

210222

102200

221200

102020

110121

201121

210210

002001

001122

201020

122010

210012

122212

011211

211211

110100

000112

210201

001011

120122

122001

222200

210020

201112

***Longest substream***: 111010000

2.2) ***Longest substream***: 0101001

2.3) ***Longest substream***: 0111001

2.4) ***Longest substream***: 1010001

2.5) ***Longest substream***: 1101110011

2.6) ***Longest substream***: 11001000

2.7) ***Longest substream***: 0100011

2.8) ***Longest substream***: 010110001

2.9) ***Longest substream***: 00000111

2.10) ***Longest substream***: 0100101

Conclusion: on average 0-1 bytes of information “survives”, however an attacker can’t predict which bytes will survive

3) Encoded base3, sanitized base3

3.1)

***Encoded secret***:

*Message*: “ȩƠĉÜ?Î##Lʺ+ūŏ`ğƨȳüɠƸôȭĕƑŭ”

*Bytes*: [553, 416, 265, 220, 63, 206, 19, 3, 76, 698, 43, 157, 363, 335, 96, 287, 151, 424, 563, 252, 608, 440, 244, 557, 277, 401, 365]

*Binary*:

202111

120102

100211

022011

002100

021122

000201

000010

002211

221212

001121

012211

111110

110102

010120

101122

012121

120201

202212

100100

211112

121022

100001

202122

101021

112212

111112

***Decoded secret***:

*Message*: “Ėʉěȸ¬ɆHȲµɽĂ#Ƿ ɱƔ˃ʖ

¬UʑkʊǛb”

*Bytes*: [278, 649, 283, 568, 172, 582, 72, 562, 181, 637, 258, 25, 503, 9, 625, 404, 707, 662, 10, 172, 85, 657, 107, 139, 650, 475, 98]

*Binary*:

101022

220001

101111

210001

020101

210120

002200

202211

020201

212121

100120

000221

200122

000100

212011

112222

222012

220112

000101

020101

010011

220100

010222

012011

220002

122121

010122

***Longest substream***: 010201012

3.2) ***Longest substream***: 10110102

3.3) ***Longest substream***: 111121210

3.4) ***Longest substream***: 010000100

3.5) ***Longest substream***: 22111111

3.6) ***Longest substream***: 12212111

3.7) ***Longest substream***: 21221010

3.8) ***Longest substream***: 0221122121

3.9) ***Longest substream***: 21000211

3.9) ***Longest substream***: 000012021

Conclusion: on average 0-1 bytes of information “survives”, however an attacker can’t predict which bytes will survive

4) for a sequence of 320

jebsmmsfzvvalkeiqwgctgsopjhyjnyj

hfksznqrzarktcwxtudolvujizaylsef

fwcahbazbdtrkemwycgupraqxabavtqg

fqzmzrfozyevftuaqponmomcdfjypunl

vvvocfthltviwmpyldogodwadvdgryiv

xjmohdeigbitgazbrfatpbosjzesbusc

tuhghbuzzesvuzjqnbwjxwvvyeudhwqt

hqlvbzsbykghztogjmpkepuqjuwssaae

lfsqzriysxoytdspvrnrrtyrfuvgccvy

smvxunsnjzrbgpomqbzhkqitfjyiypph

Longest substream: 00110100 00110100 10 ~ 2 bytes (PRNG)

Longest substream: 01010100 01101000 0110 ~ 2 bytes (CSPRNG)

5)

jebsmmsfzvvalkeiqwgctgsopjhyjnyj

hfksznqrzarktcwxtudolvujizaylsef

fwcahbazbdtrkemwycgupraqxabavtqg

fqzmzrfozyevftuaqponmomcdfjypunl

vvvocfthltviwmpyldogodwadvdgryiv

xjmohdeigbitgazbrfatpbosjzesbusc

tuhghbuzzesvuzjqnbwjxwvvyeudhwqt

hqlvbzsbykghztogjmpkepuqjuwssaae

lfsqzriysxoytdspvrnrrtyrfuvgccvy

smvxunsnjzrbgpomqbzhkqitfjyiypph

jbynndcotxuimlsqvtzdzlzmkcpwypje

gyhtzztwswpzgsheyzkwjscymmgblxqm

bggmvppufogrbhptlfryihmkuchdfhir

vedczsxhqhaxiworhehrsmhrweeryxiw

qelcuvphqgvealwkapccskxhmxquwkng

owqwhksgucuuibsauotgsohbfqchucdb

idwazfvpmpdfvzbluyhilfephwebbisn

opqpwggagvvoatqgjwjjartrcvskjism

sjpvqkkdnhozlvlegxauezzgbwqygzsd

hahxbhuwvetiwqqfrvcubargdlqabgnq