Psycho Cipher

Participants:

- Alice - Sender
- Bob - Receiver

Assumptions:

- Plaintext represents original/decrypted message.
- Ciphertext represents encrypted message.
- The key is used to encrypt the plaintext.
- Key is known to both sender and receiver. (symmetric)
- There are only alphabets which are used as plaintext letters.
- Noise bit 0

Key Formation:

- The key is dynamic. It will be calculated as follows.
    - Number of plaintext letters = N
    - Bits per alphabet = 7
    - total bits = N * 7
    - key length = sqrt (total bits) + 1

  For eg.

  Plaintext = ABC N = 3
  Bits = 100000110000101000011
  N * 7 = 21
  sqrt(21) = 4
  Key Length = 4 + 1 = 5
  Key = 97531 (distinct digits upto length 9, after that key will be repeated)

Encryption:

Letters = ‘HELLO’

In bits = ‘100100\010001\011001\100100\110010\01111’

Key length = 6

Random key = 240153

Random key in bits

- 2 = 0110010
- 4 = '0110100'
- 0 = '0110000’
- 1 = '0110001'
- 5 = '0110101'
- 3 = '0110011'

How to encrypt message : **Layer 1**

1	0	0	1	0	0
0	1	0	0	0	1
0	1	1	0	0	1
1	0	0	1	0	0
1	1	0	0	1	0
0	1	1	1	1	0(noise)

Now Distribute Key:

1(2)	0	0	1	0	0
0	1(4)	0	0	0	1
0	1	1(0)	0	0	1
1	0	0	1(1)	0	0
1	1	0	0	1(5)	0
0	1	1	1	1	0(noise)(3)

Layer 2.a:

1(2) →	0 →	0 →	1 →	0 →	0 →
0	1(4) →	0 →	0 →	0 →	1 →
0	1	1(0) →	0 →	0 →	1 →
1	0	0	1(1) →	0 →	0 →
1	1	0	0	1(5) →	0 →
0	1	1	1	1	0(noise)(3)→

Write Encrypted message after layer 2.a:
Order : Blue, Brown, Orange, Magenta, Red, Green
10011001001000100011

Layer 2.b:

1(2)	0	0	1	0	0
0→	1(4)	0	0	0	1
0→	1→	1(0)	0	0	1
1→	0→	0→	1(1)	0	0
1→	1→	0→	0→	1(5)	0
0→	1→	1→	1→	1→	0(noise)(3)

Write Encrypted message after layer 2.b:
Order : Blue, Brown, Magenta, Red, Green
011000111101100

Write Encrypted message after layer 2:
10011001001000100011001100011110110011

Layer 3: (Depends on Security Inspector)
(2) + H + (4) + E + (0) + L +(1) + L + (5) + O + (3)

Complexity of the algorithm:
For eg : N = 21
Void spaces = 22
Key Length = sqrt(21 * 7) + 1 = 13
Ways of Distribution : 22 Permute in 13
Probability of trudy getting right = 1 / ways

Length equation for Receiver / Trudy :

- (total length + Key Length) * 7

Decryption:

- Recover Key
- Extract (ciphertext - encrypted key)
- Arrange in the form of matrix of dim key length * key length
- Number the diagonal of matrix as per the key
- Reverse layer 2 encryption.