

**Solution:**

**Let’s assume:**

**L > Unicity distance of the substation cipher**

**C > Corresponding ciphertext**

**When n! possible key the probability of guessing key is 1/n!**

**There are 2 cases for this. One when the length of Ciphertext ( c) <L [ result: more possible plaintexts]**

**Other, length of the ciphertext (c) > L**

**For estimating unicity of substitution cipher,**

**When the length of the given ciphertext k , the possible plaintext are:**

**n(n-1)(n-2)(n-3)…..(n-k+1)**

**when n is larger than k then value becomes nK.**

**Now,**

**Suppose ciphertext= L**

**Possible plaintext nL but if N is larger than L**

**n! =** ≈ √(2πn) \* (n/e)n

**adding log on both sides,**

log(n!) ≈ log(√(2πn) \* (n/e)n)

log(n!) ≈ 1/2log(2πn) + n log (n/e)

**we know** log(xy) = y\* log (x) so,

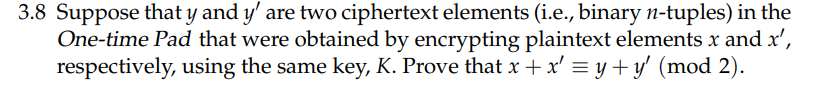
log(n!) ≈ 1/2log(2πn) + nlog(n) –n

Solving for L,

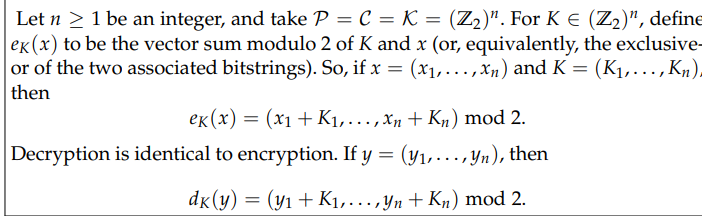
L ≈ (1/2log(2πn) + nlog(n) –n ) /log(n)

So,

L ≈ (1/2log(2πn) + nlog(n) – n) / log(n)



Here as we know,



Given.

Plaintext: x and x’

cipher text after encrypting,

y = x + K ----1

y’ = x’ + K ----2, where + denotes X-OR operation

From 1 and 2 equation we get,

y + y’ = (x + K )+ (x’ + K)

y + y’ = x + x’ + 2K

K denotes tuple, also

2K ≡ 0 (mod2) as binary tuple addition with itself =0

We get,

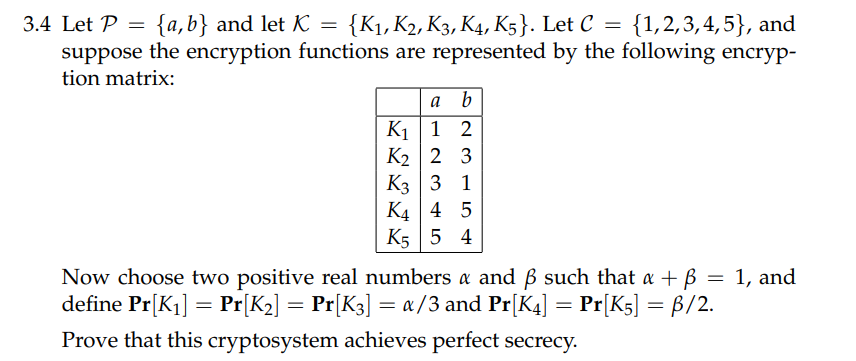
y + y’ ≡ x + x’ (mod2)

i,e,

X-OR of (y and y’ equivalent to x and x’)mod 2

Also, if we (add plaintext of x and x’ equivalent to adding the ciphertext of y and y’ bitwise) modulo 2

Hence, proved.



Here,

Suppose,

α = 0.6

β= 0.4

α + β = 1

0.6+ 0.4 =1

Hence,

Pr [K1] = Pr [K2] = Pr [K3] = α/3 = 0.6/3 = 1/5

And, Pr [K4] = Pr [K5] = β/2 = 0.4/2 = 1/5

Pr[a] + Pr[b] = 1

Pr[a] = 1/5

and     Pr[b] = 4/5

**Pr[y]  = ∑Pr(k) \* Pr(dk ( y))**

Now,

Pr[1] = (Pr[a] \* Pr[K1]) + (Pr[b] + Pr[K3])

                = (1/5 \* 1/5) + (4/5 \* 1/5) = 1/25 + 4/25 = 5/25 = 1/5

Pr[2] = (Pr[a] \* Pr[k2]) + (Pr[b] \* pr[K1])

         = (1/5 \* 1/5) + (4/5 \* 1/5) = 1/25 + 4/25 = 5/25 = 1/5

Pr[3] = (Pr[a] \* Pr[k3]) + (Pr[b] \* pr[K2])

          = (1/5 \* 1/5) + (4/5 \* 1/5)  = 1/5

Pr[4] = (Pr[a] \* Pr[k4]) + (Pr[b] \* pr[K5])

         = (1/5 \* 1/5) + (4/5 \* 1/5) = 1/5

Pr[5] = (Pr[a] \* Pr[k5]) + (Pr[b] \* pr[K4])

         = (1/5 \* 1/5) + (4/5 \* 1/5)  = 1/5

Now, P[1] + P[2] + P[3] + p[4] +[5] =1

As 1/5 + 1/5 + 1/5 + 1/5 + 1/5 = 1

**Perfect secrecy achieved when**

**A posteriori probabilities = a priori probabilities**

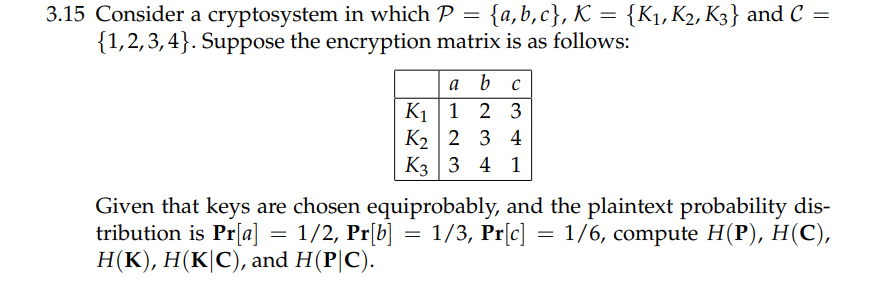
**Pr[x | y]  =  Pr[x] for x € P and y € C**

**Pr[x | y] = (Pr[x] \* pr[y | x]) / Pr[y]**

Where    **Pr[y | x ] =** {k:dky=x}Pr[K]

                          = 1/5+ 1/5 +1/5 + 1/5 + 1/5 = 1

**Pr[x] = (1/5 \* 1)/(1/5) = 1**



Here,

**H(P|C) = H(P, C) − H(C)**  
Since,

Pr[a] = 1/2,

Pr[b] = 1/3,

Pr[c] = 1/6.

Also,  
**H(P) =** 1/2 log22 + 1/3 log23 + 1/6 log26 = 2/3 + 1/2 log23**≈ 1.459**

**Now,  
Calculation of probability Distribution of C**

Pr[y = 1] = 2/9,

Pr[y = 2] = 5/18,

 Pr[y = 3] = 1/3,

 Pr[y = 4] = 1/6

**Hence, entropy of the ciphertext:**

**H(C) =**−2/9 log22/9 − 5/18 log25/18 − 1/3 log21/3 − 1/6 log21/6**≈ 1.955.  
  
Since,**  
Pr[x = a, y] = 1/6 , for y = 1, 2, 3  
Pr[x = b, y] = 1/9 , for y = 2, 3, 4  
Pr[x = c, y] = 1/18 , for y = 1, 3, 4

**Remaining 3 probabilities are 0 so,  
H(P, C) =** 3 × [1/6 log26 + 1/9 log29 + 1/18 log218]**≈ 3.044,**

**Hence,**

**H(P|C) =** H(P, C) − H(C) = 3.044 - 1.955**≈ 1.089.**