Class Notes 2/16/17

David Rogers

March 8, 2017

Starting from where last class left off;

$(P(message =' YES') * P(key = K2))/(P(key = K1) * P(message =' NO') + P(Key = K2) * P(message =' YES'))$

What we get from the tables mentioned last class is:

$((1/4) * (1/3))/((1/3) * (3/4) + (1/4) * (1/3)) = 1/4$ so Eve didnt learn anything.

What if eve captures 7 instead?

Eve knows something then. A cryptosystem has perfect secrecy if for any ciphertext 'C' and any message 'M' P(message in 'M' | Ciphertext 'C') = P(message is'M')

DOWNSIDES: Alice and Bob have to share the key, they can only use it once .

Theorem: The one-time-pod has perfect secrecy

The next part is just showing different short cuts how to find the GCD of numbers much faster.

1. Compute GCD(6,9)=3 2. factor m,n take prime powers that divide both

GCD(12,30)=6
12=2*2*3
30=2*3*5

so group the 2*3 which both have in common and you have 6
3. This is the fast method: Euclids algorithm
GCD(M,N)=d
d divides (m-n)
d divides (m-a*n)

Use division with remainder

n/m=a with remainder r

d still divides r

GCD(m,n)= GCD(n,r)

Ex. GCD(1317,56)

is simplified to GCD(56,29) which is obtained by dividing 56/1317

This gives you remainer 29

Then divide 29/56 which gives you remainder 27

So the GCD(29,27

) You keep repeating this process until the divisor is 1 or cannot be simplified any further.