



all it work in binary, must convert from ascii or number to binary

**KSA**

**Input key, key\_length**

**Output: permuted s-box**

**Init s-box 256 element from 0-255**

**Init T array use key input fill out 0 -255**

**Loop 0 -> 255**

**Set j = (j+S[i]+T[i]) mod 256**

**Swap S[i] with S[j]**

**Return S**

**PRGA**

**Input: s-box(S)**

**Output: keystream**

**Init I,j=0**

**While(byte to encrypt) do // length plaintext**

**I = i+1, j = (j+S[i])**

**Swap S[i] with S[j]**

**Update** k = (S[i]+S[j]) mod 256

output S[k]

end while

**https://core.ac.uk/download/pdf/82782454.pdf**