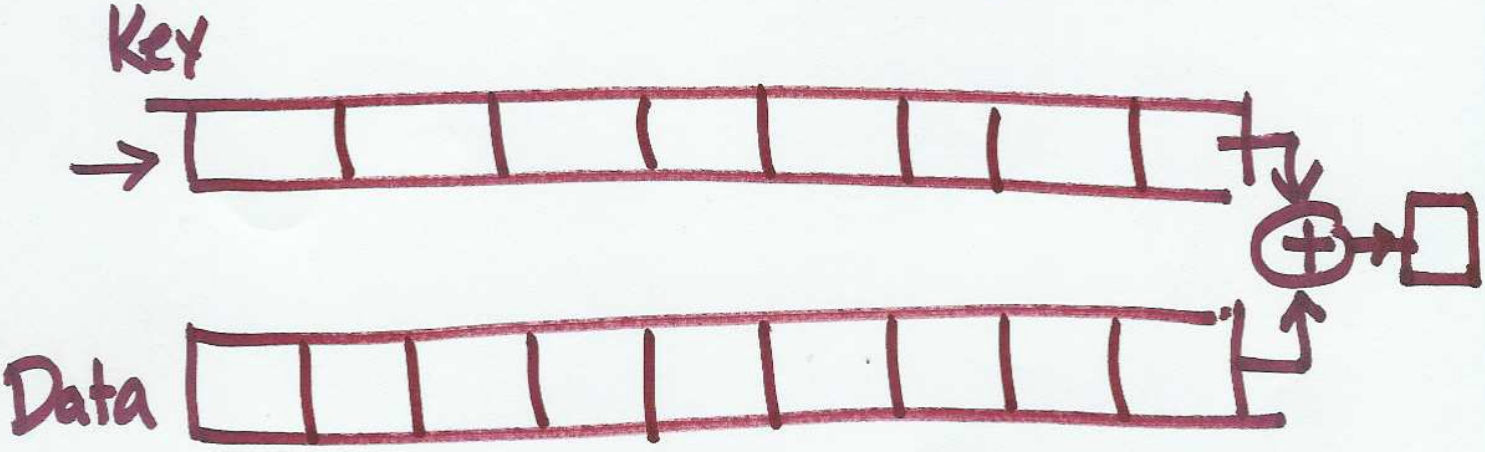
2/8/07

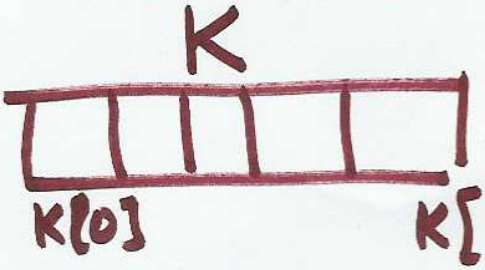
RC 4

stream cipher



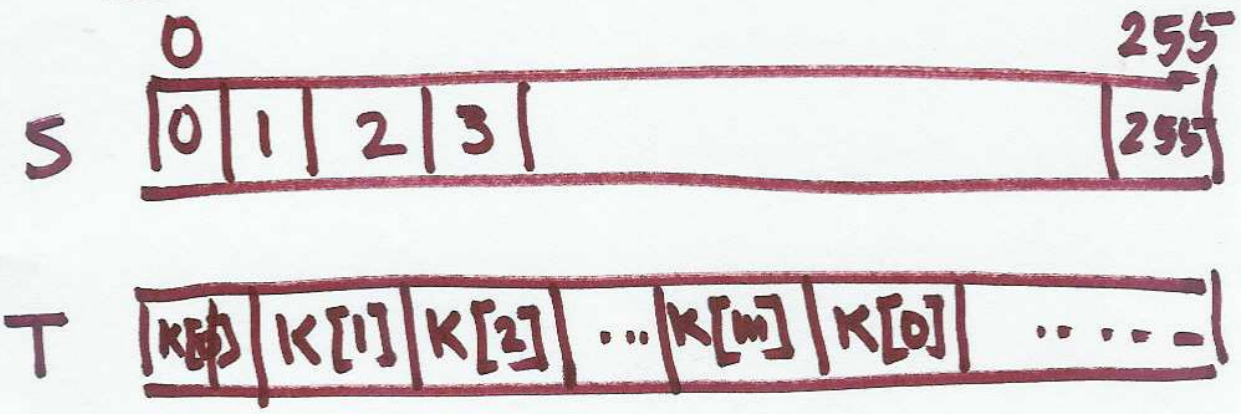
How do you generate K?

Secret



. Keylength

Initialization

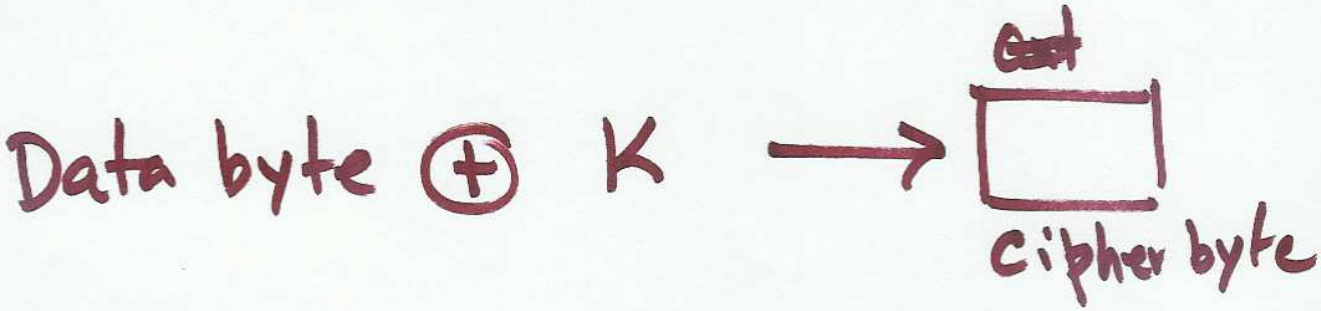


Initial Permutation of S

```
j = 0
for i = 0 to 255 do
    j = (j + S[i] + T[i]) mod 256;
    swap( S[i], S[j] );
```

Stream Generation

```
i, j = 0
while (true)
  i = (i+1) mod 256
  j = (j + S[i]) mod 256
  swap (S[i], S[j])
  t = (S[i] + S[j]) mod 256
  K = S[t]
```



802.11 i

IEEE — Wi-Fi Alliance

802.11 — Wi-Fi Product

No. Encrypt, WEP — No Encrypt + WEP + Modified WEP

TKIP ← RC4 → WPA

RSN — WPA2

Authentication Server → RADIUS

Access Control — IEEE 802.1X

Wireless LAN