Cryptography and Network Security Chapter 7

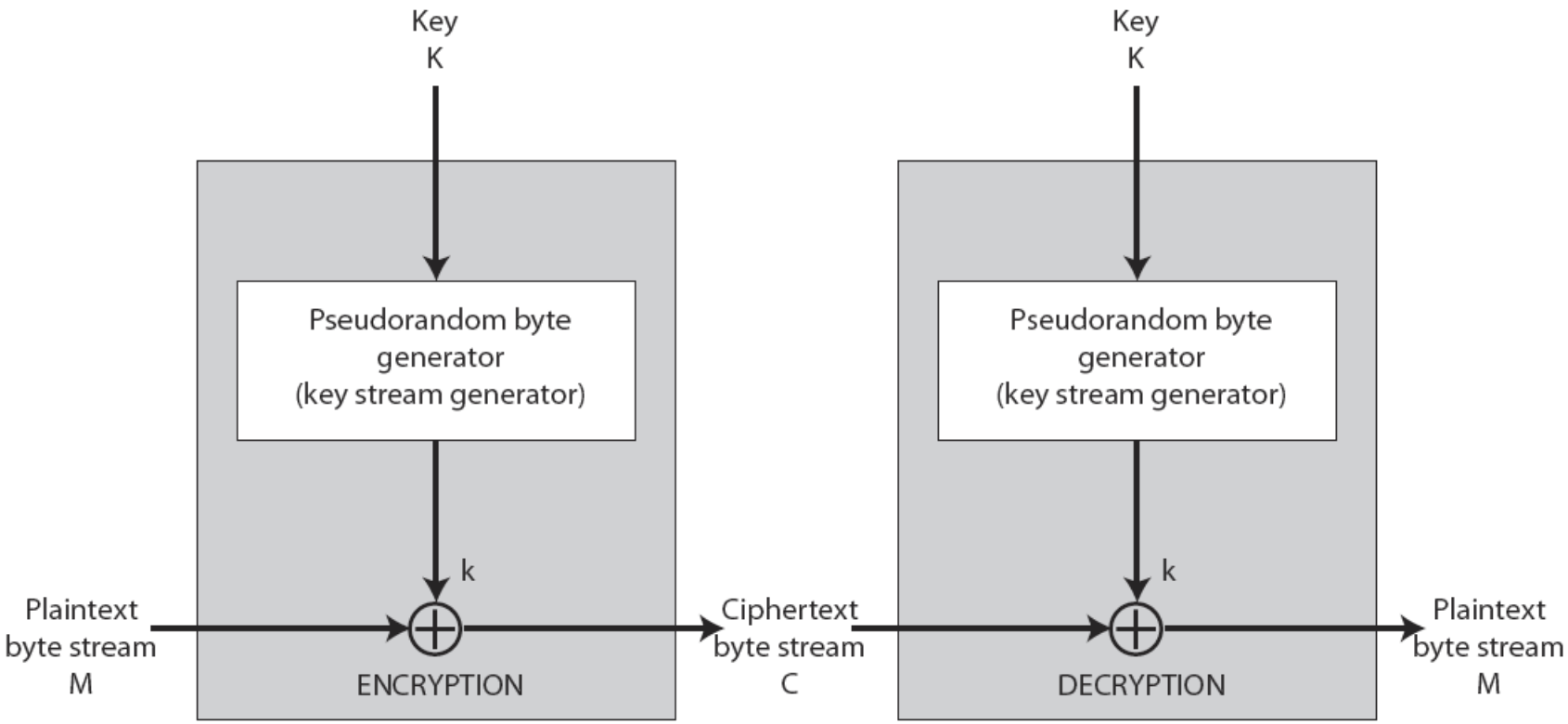
Fifth Edition

by William Stallings

Κρυπτογραφικοι Αλγοριθμοι Ροής (Stream Ciphers)

- Επεξεργαζονται το μηνυμα bit προς bit (σαν μια ροη)
- Εχουν ένα ψευδοτυχαίο **keystream**
- Το keystream συνδιάζεται (γίνεται XOR) με το h plaintext bit προς bit
- Η τυχαιότητα του **keystream** καταστρεφει τελείως τις στατιστικες ιδιοτητες του μηνυματος
  - $C_i = M_i$ XOR $Keystream_i$
- Δεν πρεπει ποτε να επαναχρησιμοποιουμε το keystream
  - Αλλιώς μπορει να αποκαλυφθουν τα μηνυματα

Δομη ενος Αλγοριθμου Ροης (Stream Cipher Structure)



Ιδιοτητες του Αλγοριθμου Ροης (Stream Cipher Properties)

- σχεδιαστικες προϋποθεσεις:
  - Μακρα περιοδος χωρις επαναληψεις
  - Στατιστικα Τυχαιος
  - Βασιζεται σε επαρκως μεγαλο κλειδι
  - Μεγαλη γραμμικη πολυπλοκοτητα
- Αν σχεδιαστει σωστα, μπορει να ειναι ασφαλης οσο και ενας αλγοριθμος τμηματων με το ιδιο μεγεθος κλειδιου
- Αλλα ειναι συνηθως απλουστερος και ταχυτερος

RC4

- Ειναι ενας ιδιωτικος κρυπτογραφικος αλγοριθμος που ανηκει στην RSA DSI
- Εχει σχεδιαστει κι αυτος απο τον Ron Rivest
- Η σχεδιαση του ειναι απλη αλλα αποτελεσματικη
- Εχει μεταβλητο μεγεθος κλειδιου, ειναι ενας byte-oriented κρυπτογραφικος αλγοριθμος ροης
- Χρησιμοποιειται ευρυτατα (web SSL/TLS, wireless WEP/WPA)

RC4 Key Schedule

- Αρχιζει με ενα array S με αριθμους: 0..255
- Χρησιμοποιουμε το κλειδι για να ανακατεψουμε καλα
- Το S σχηματιζει την εσωτερικη κατασταση του αλγοριθμου

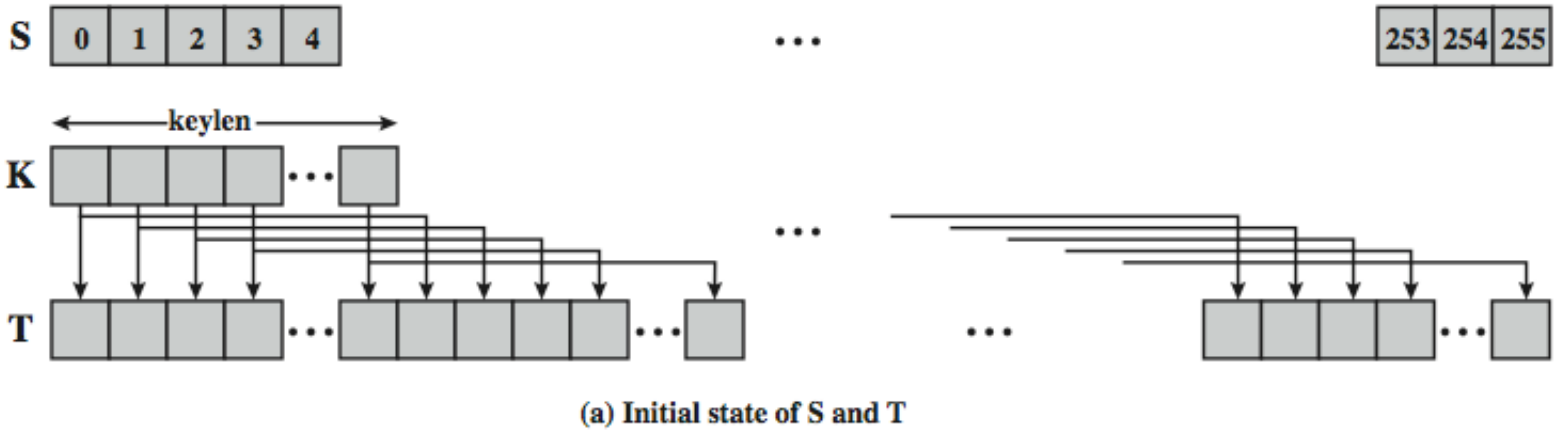
```
for i = 0 to 255 do
   S[i] = i
   T[i] = K[i mod keylen])
j = 0
for i = 0 to 255 do
   j = (j + S[i] + T[i]) (mod 256)
   swap (S[i], S[j])
```

RC4 Encryption

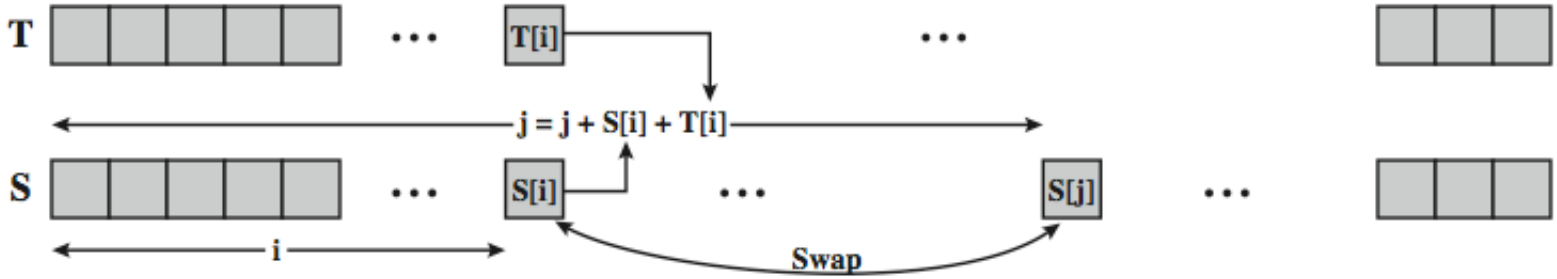
- Η κρυπτογραφηση συνεχιζεται ανακατευοντας τις τιμες του array
- Το αθροισμα του ανακατεμενου ζευγους επιλεγει την τιμη του "stream key" απο τη μεταθεση.
- Κανουμε XOR το S[t] με το επομενο byte του μημυματος για να κρυπτογραφησουμε /αποκρυπτογραφησουμε

```
i = j = 0
for each message byte M_i
   i = (i + 1) (mod 256)
   j = (j + S[i]) (mod 256)
   swap(S[i], S[j])
   t = (S[i] + S[j]) (mod 256)
   C_i = M_i XOR S[t]
```

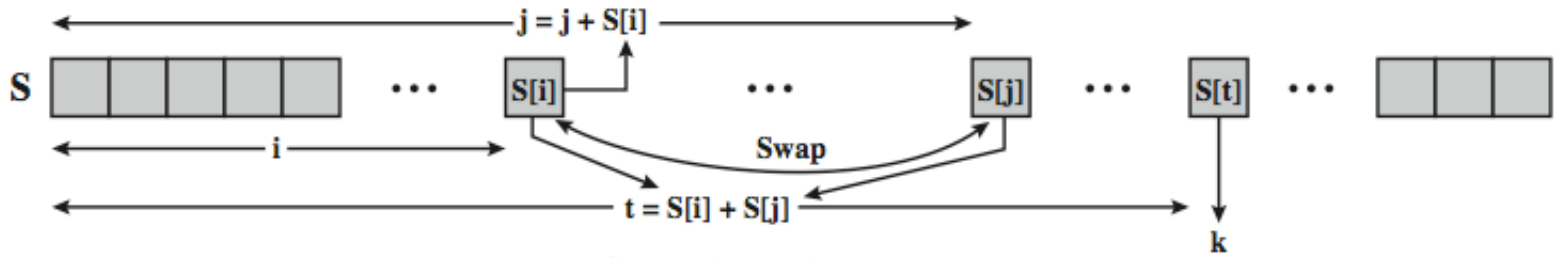
RC4 Overview



(a) Initial state of S and T



(b) Initial permutation of S



(c) Stream Generation

Ασφαλεια του RC4

- λεγεται οτι ειναι ασφαλης εναντι των γνωστων επιθεσεων.
  - Υπαρχουν καποιες προσπαθειες κρυπταναλυσης, αλλα καμια δεν ειναι πρακτικη
- Το αποτελεσμα ειναι πολυ μη γραμμικο.
- Επειδη ο RC4 ειναι αλγοριθμος ροης δεν πρεπει ποτε να επαναχρησιμοποιειται το κλειδι.
- Υπαρχει ενα προβλημα με το WEP, αλλα λογω της διεχειρισης του κλειδιου και οχι του ιδιου του RC4

Συνοψη

- Κρυπτογραφικοι αλγοριθμοι ροης.
- Ο Αλγοριθμος RC4