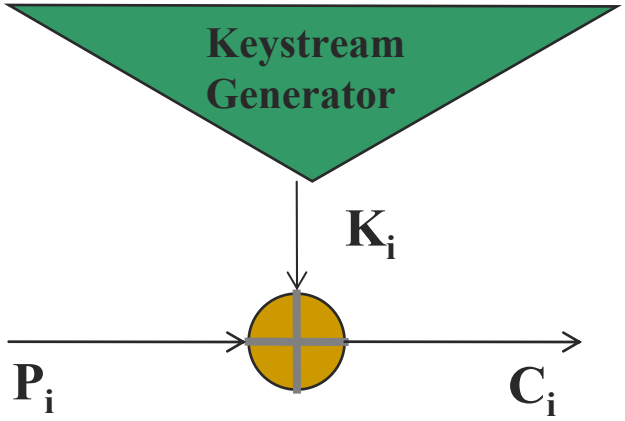
Κρυπτογραφία

Εργαστηριακό μάθημα 5

Stream ciphers –

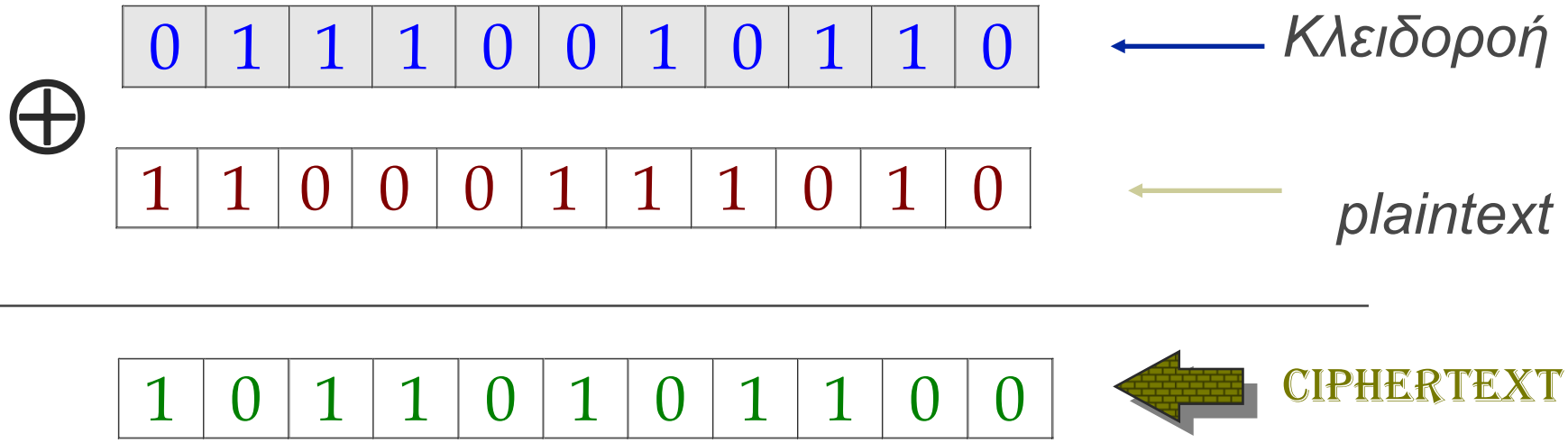
Κρυπτανάλυση με τον αλγόριθμο Berlekamp-Massey

Γενικά χαρακτηριστικά των stream ciphers



- Δουλεύουν πάνω σε ένα ρεύμα από bits (ή bytes)
- Απαιτούν μία γεννήτρια ψευδοτυχαίας ακολουθίας bits (keystream generator) – αυτή η ακολουθία που παράγεται λέγεται κλειδοροή (keystream)
- Τα bits του κλειδιού γίνονται XOR με τα bits του μηνύματος για να προκύψει έτσι το κρυπτόγραμμα, δηλαδή $c_i = p_i \oplus k_i$
- Η αποκρυπτογράφηση γίνεται με τον ίδιο τρόπο (ο παραλήπτης έχει την ίδια γεννήτρια κλειδοροής, και κάνει XOR το κάθε bit κρυπτογράμματος με το αντίστοιχο bit της κλειδοροής) $p_i = c_i \oplus k_i$
- Η περίοδος της κλειδοροής πρέπει να είναι όσο γίνεται πιο μεγάλη

Παράδειγμα λειτουργία stream ciphers



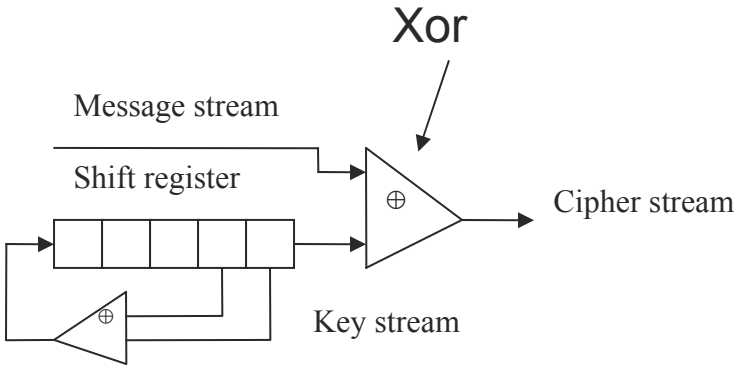
Σημείωση: Λειτουργία του τελεστή XOR ⊕ :

- *a ⊕ b = 0 αν τα a,b είναι ίδια,*
- *a ⊕ b = 1 αν τα a,b είναι διαφορετικά.*

Αντίστοιχα, για πολλές μεταβλητές (π.χ. a ⊕ b ⊕ c ⊕ …..), αν άρτιος αριθμός από αυτές είναι 1 τότε το αποτέλεσμα είναι 1, αλλιώς το αποτέλεσμα είναι 0.

Τι είναι τα συστήματα παραγωγής κλειδοροής στην πράξη?

- Ως γεννήτρια ψευδοτυχαίων bits χρησιμοποιήθηκε αρχικά ένας **γραμμικός καταχωρητής ολίσθησης με ανάδραση (LFSR)**
- Έχουν καλή μαθηματική περιγραφή και οι ιδιότητές τους αναλύονται εύκολα

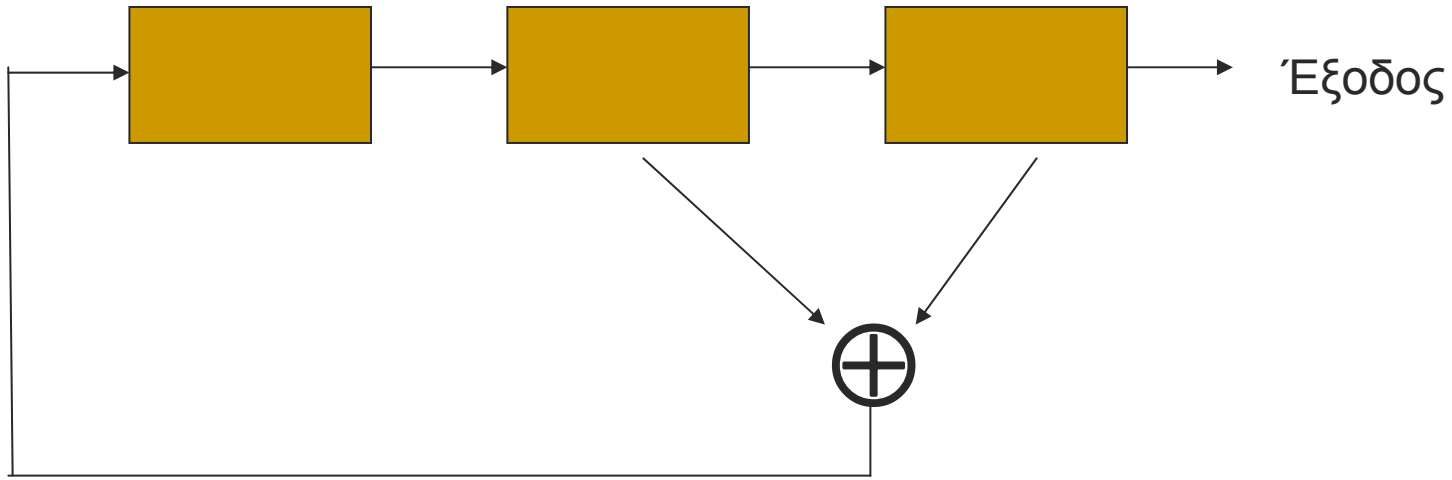


Λειτουργία ενός LFSR

- Αποτελείται από Ν βαθμίδες (θέσεις μνήμης): το περιεχόμενο κάθε μιας είναι είτε 0 είτε 1. Κάποιες από τις βαθμίδες αυτές γίνονται xor και το αποτέλεσμα πηγαίνει πίσω στην πρώτη βαθμίδα. Αν ο LFSR βρίσκεται σε μία κατάσταση (δηλαδή οι βαθμίδες του έχουν μία συγκεκριμένη τιμή), τότε η επόμενη κατάστασή του προσδιορίζεται εύκολα από τον ακόλουθο κανόνα:
  - Όλες οι βαθμίδες (η τιμή τους δηλαδή) ολισθαίνουν κατά μία θέση δεξιά
  - Η νέα τιμή για την πρώτη βαθμίδα είναι το αποτέλεσμα της παραπάνω XOR πράξης

Σχηματική αναπαράσταση της λειτουργίας ενός LFSR

Παράδειγμα: LFSR τριών βαθμίδων



Αν η αρχική κατάσταση είναι 001, τότε η έξοδος είναι 1 (η δεξιότερη βαθμίδα).

Την επόμενη χρονική στιγμή, η κατάσταση θα είναι 100 και η έξοδος 0. Το 100 προκύπτει ως εξής: το «1» είναι το XOR που είχαν αρχικά η δεύτερη και η τρίτη βαθμίδα (που ήταν 0 και 1 αντίστοιχα), ενώ το «00» είναι απλά ολισθημένες οι τιμές που είχαν αρχικά η πρώτη με τη δεύτερη βαθμίδα.

Σχηματική αναπαράσταση της λειτουργίας ενός LFSR (II)

- Στον προηγούμενο LFSR, αν θεωρήσουμε ότι η αρχική κατάσταση είναι η 001, οι διαδοχικές καταστάσεις από τις οποίες περνάει (και η αντίστοιχη έξοδος που παράγεται) είναι:

Κατάσταση	**Έξοδος**
00**1**	**1**
10**0**	**0**
01**0**	**0**
10**1**	**1**
11**0**	**0**
11**1**	**1**
01**1**	**1**
00**1**	**1**

Η 001 έχει ξαναεμφανιστεί, οπότε οι καταστάσεις επαναλαμβάνονται. Άρα, ο συγκεκριμένος LFSR παράγει την ακολουθία 1001011, η οποία επαναλαμβάνεται περιοδικά

Ιδιότητες LFSRs

- Ένα LFSR μήκους L μπορεί να περάσει από 2^L -1 διαφορετικές καταστάσεις, άρα μπορεί να γεννήσει ακολουθίες με μέγιστη περίοδο 2^L -1.
- Γενικά, η ακολουθία εξόδου ενός LFSR εξαρτάται τόσο από την ανάδρασή του όσο και από την αρχική του κατάσταση.
- Στην πράξη προτιμούμε LFSRs που περνάνε από όλες τις καταστάσεις, έτσι ώστε η παραγόμενη κλειδοροή να έχει τη μέγιστη δυνατή περίοδο.
- Σημαντική ιδιότητα: ακολουθίες περιόδου 2^L -1 που παράγονται από LFSRs μήκους L (για οποιαδήποτε τιμή του L) παρουσιάζουν πολύ καλά χαρακτηριστικά ψευδοτυχαιότητας (εκτός από τη μεγάλη περίοδο) – άρα, αυτοί οι LFSRs δείχνουν να είναι ιδανική επιλογή

Berlekamp – Massey αλγόριθμος (κρυπτανάλυση)

- Ο ελάχιστος LFSR που μπορεί να παράγει μία δοθείσα ακολουθία υπολογίζεται γρήγορα με τον αλγόριθμο Berlekamp-Massey.
- **Αν το μήκος του μικρότερου LFSR που παράγει μία ακολουθία είναι L, τότε ο Berlekamp-Massey χρειάζεται μόνο 2L διαδοχικά bits της ακολουθίας για να υπολογίσει αυτόν τον ελάχιστο LFSR!!**
- Συμπέρασμα: Οι ακολουθίες που παράγονται από LFSRs μπορούν εύκολα να προβλεφτούν!!
  - Παράδειγμα: Έστω L=128. Τότε, παράγουμε μία ακολουθία περιόδου 2^{128}-1 (που είναι πολύ μεγάλη). Ωστόσο, αν ξέρουμε μόνο 256 διαδοχικά bits της ακολουθίας τότε βρίσκουμε επακριβώς τον LFSR αυτόν – άρα, ολόκληρη την ακολουθία!
  - Μπορούμε να γνωρίζουμε ποτέ ένα τμήμα της κλειδοροής, έτσι ώστε κάνοντας χρήση του Berlekamp-Massey να τη βρίσκουμε ολόκληρη?
    - Ναι!! Αν ξέρουμε ένα μικρό τμήμα του μηνύματος, τότε ουσιαστικά ξέρουμε το αντίστοιχο τμήμα της κλειδοροής!!

Berlekamp – Massey αλγόριθμος (Περιγραφή)

Input: $s^n = s_0 s_1 s_2 \ldots s_{n-1}$
$C(x) = 1; L = 0; m = -1; B(x) = 1; N = 0;$ // initialize
while ($N < n$) {
    $d = (s_N + \sum_{i=1,L} c_i s_{N-i}) \bmod 2;$ // next discrepancy

    if ($d == 1$) { // update LFSR
        $T(x) = C(x); C(x) = C(x) + B(x)*x^{N-m};$
        if $L \leq N/2$ {
            $L = N+1-L; m = N; B(x) = T(x);$
        }
    }
    ++N;
}
return(L,C);

Berlekamp – Massey αλγόριθμος (Παράδειγμα)

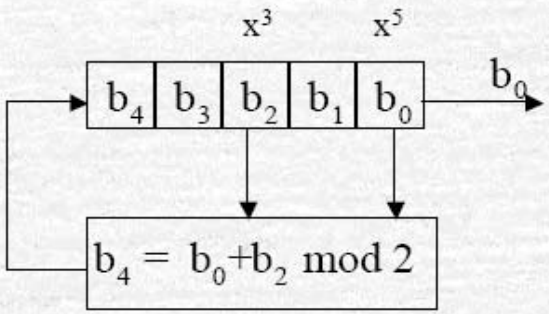
Given:

$s^n = 001101110$, $n = 9$

Output:

Polynomial: $1+x^3+x^5$

Can determine:



Initial state 00110

values at end of each while loop iteration

s_n	d	T(x)	C(x)	L	m	B(x)	N
-	-	-	1	0	-1	1	0
0	0	-	1	0	-1	1	1
0	0	-	1	0	-1	1	2
1	1	1	$1+x^3$	3	2	1	3
1	1	$1+x^3$	$1+x+x^3$	3	2	1	4
0	1	$1+x+x^3$	$1+x+x^2+x^3$	3	2	1	5
1	1	$1+x+x^2+x^3$	$1+x+x^2$	3	2	1	6
1	0	$1+x+x^2+x^3$	$1+x+x^2$	3	2	1	7
1	1	$1+x+x^2$	$1+x+x^2+x^5$	5	7	$1+x+x^2$	8
0	1	$1+x+x^2+x^5$	$\mathbf{1+x^3+x^5}$	5	7	$1+x+x^2$	9

$N = 4$, $L = 3$: $C(x) = c_1 s_2 + c_2 s_1 + c_3 s_0 = 1*1+0*0+1*0 = 1$

$s_4 = 0 \neq C(x)$, so set $d = 1$

Πηγή: http://www1.cs.columbia.edu/~tal/4995/