



ΙΟΝΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ

ΓΕΝΝΗΤΡΙΕΣ ΤΥΧΑΙΩΝ ΑΡΙΘΜΩΝ

ΠΛΑΤΑΝΙΑΣ ΘΕΟΔΩΡΟΣ Π2011002

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ: ΑΥΛΩΝΙΤΗΣ ΜΑΡΚΟΣ





ΠΕΡΙΕΧΟΜΕΝΑ

1. ΟΡΙΣΜΟΣ ΤΥΧΑΙΟΤΗΤΑΣ
2. ΟΡΙΣΜΟΣ ΓΕΝΝΗΤΡΙΩΝ ΤΥΧΑΙΩΝ ΑΡΙΘΜΩΝ
3. ΠΡΑΓΜΑΤΙΚΕΣ & ΨΕΥΔΟΤΥΧΑΙΕΣ ΓΕΝΝΗΤΡΙΕΣ
4. ΣΥΓΚΡΙΣΗ PRNG ΚΑΙ TRNG
5. ΠΑΡΑΔΕΙΓΜΑΤΑ ΨΕΥΔΟΤΥΧΑΙΩΝ ΓΕΝΝΗΤΡΙΩΝ
6. ΠΡΟΓΡΑΜΜΑ SLOT MACHINE



ΤΙ ΕΙΝΑΙ ΤΥΧΑΙΟ ?

ΟΡΙΣΜΟΣ 1 (LEIBNIZ): Κάτι μπορεί να οριστεί ως τυχαίο όταν η μαθηματική εξίσωση που το περιγράφει είναι περίπλοκη σε μεγάλο βαθμό.

ΟΡΙΣΜΟΣ 2 (SHANNON): Η τυχειότητα είναι αντίθετη από τον ντετερμινισμό σε μια στοχαστική διαδικασία. Με αποτέλεσμα αν ένα σύστημα έχει εντροπία μηδέν , δεν έχει τυχειότητα και η αύξηση της εντροπίας οδηγεί σε αύξηση της τυχειότητας.

ΓΕΝΝΗΤΡΙΕΣ ΤΥΧΑΙΩΝ ΑΡΙΘΜΩΝ



ΟΡΙΣΜΟΣ: Μια γεννήτρια τυχαίων αριθμών είναι μια υπολογιστική ή μηχανική συσκευή που έχει σχεδιαστεί για να παράγει μια ακολουθία αριθμών ή συμβόλων που δεν ακολουθούν κάποιο μοτίβο, δηλαδή εμφανίζονται τυχαία.

ΕΦΑΡΜΟΓΕΣ: Τυχικά παιχνίδια, Κρυπτογραφία, δειγματοληψία για στατιστικές κ.λ.π.

ΠΡΑΓΜΑΤΙΚΕΣ ΚΑΙ ΨΕΥΔΟΤΥΧΑΙΕΣ ΓΕΝΝΗΤΡΙΕΣ



TRNG: Εισάγει τα φυσικά φαινόμενα που υπάρχουν στο πραγματικό κόσμο στον υπολογιστή και παράγει στην έξοδο πραγματικά τυχαίους , ανεξάρτητους και απρόβλεπτους αριθμούς.

PRNG: Στηρίζονται στην ύπαρξη ενός ή περισσότερων ντετερμινιστικών αλγορίθμων για την παραγωγή των νέων κάθε φορά αριθμών.

ΔΙΑΦΟΡΕΣ PRNG & TRNG

ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ	PRNG	TRNG
ΑΠΟΔΟΤΙΚΟΤΗΤΑ	ΥΨΗΛΗ	ΧΑΜΗΛΗ
ΝΤΕΤΕΡΜΙΝΙΣΜΟΣ	ΝΤΕΤΕΡΜΙΝΙΣΤΙΚΗ	ΜΗ ΝΤΕΤΕΡΜΙΝΙΣΤΙΚΗ
ΠΕΡΙΟΔΙΚΟΤΗΤΑ	ΠΕΡΙΟΔΙΚΗ	ΑΠΕΡΙΟΔΙΚΗ
ΚΟΣΤΟΣ	ΧΑΜΗΛΟ	ΥΨΗΛΟ

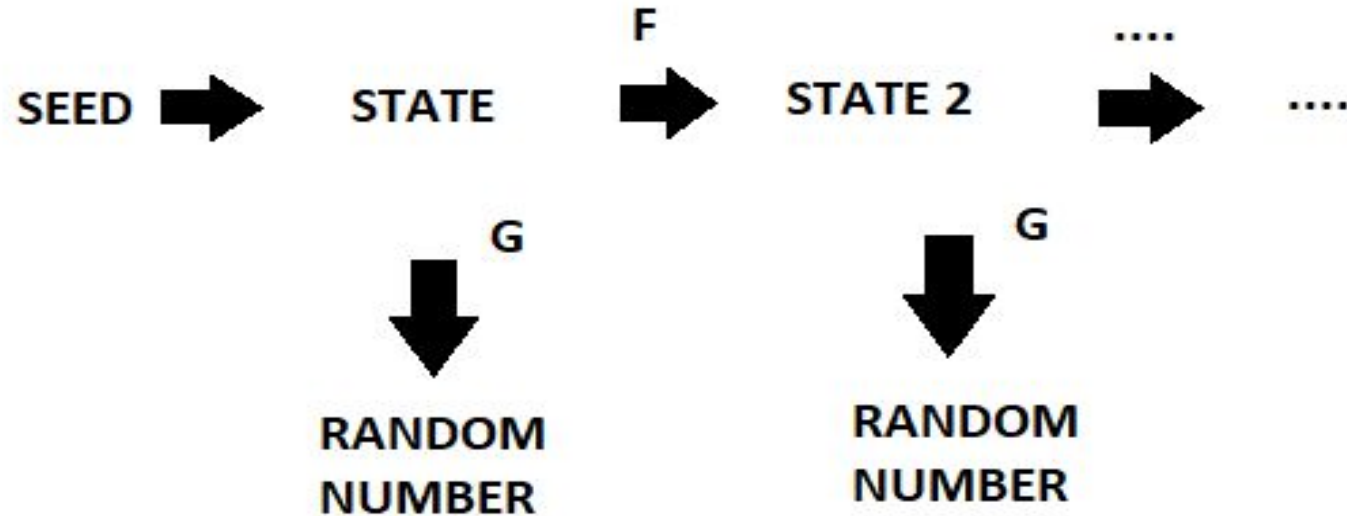


ΣΠΟΡΟΣ ΚΑΙ ΠΕΡΙΟΔΙΚΟΤΗΤΑ

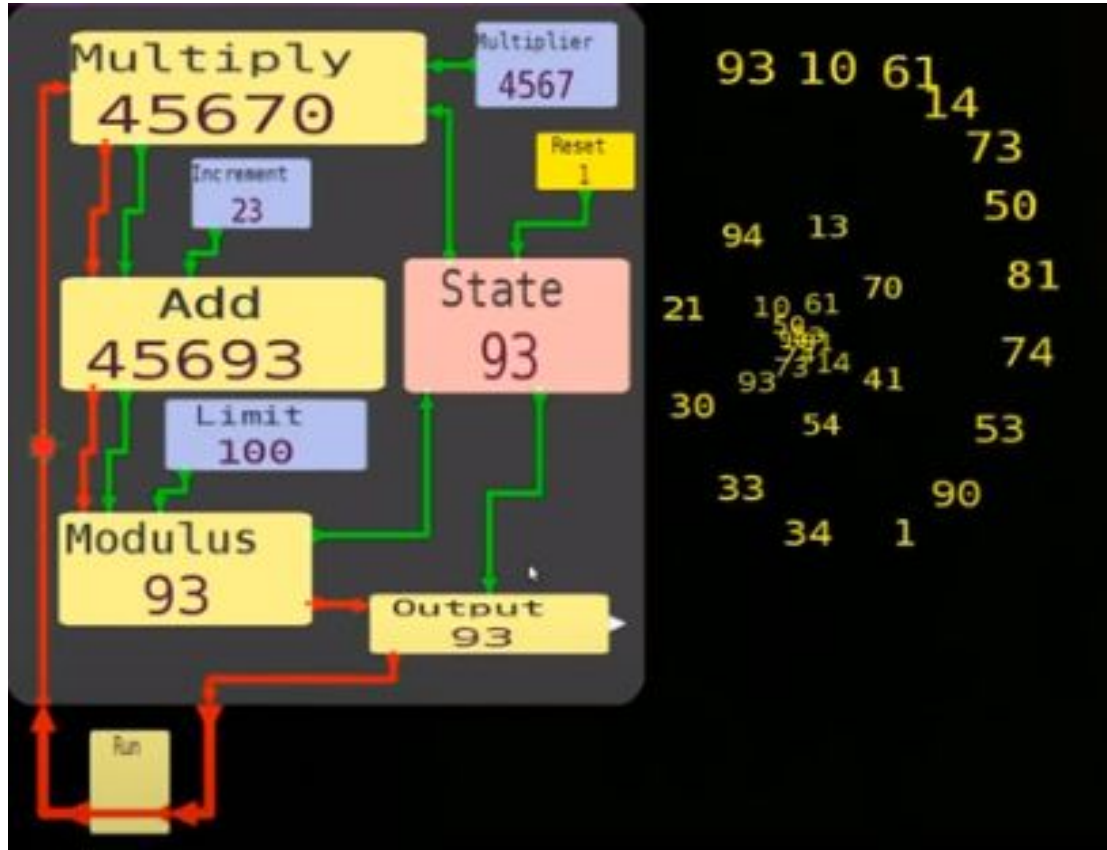
Το μήκος της ακολουθίας αριθμών που παράγεται από τη κάθε γεννήτρια χωρίς να περιλαμβάνει κάποιον επαναλαμβανόμενο αριθμό ονομάζεται περίοδος ή κύκλος της γεννήτριας

Το σύνολο των τιμών που δέχεται η κάθε γεννήτρια ως είσοδο για να αρχίσει η διαδικασία παραγωγής ονομάζεται σπόρος (seed).

ΓΕΝΝΗΤΡΙΕΣ ΨΕΥΔΟΤΥΧΑΙΩΝ ΑΡΙΘΜΩΝ



LINEAR CONGRUENTIAL GENERATOR

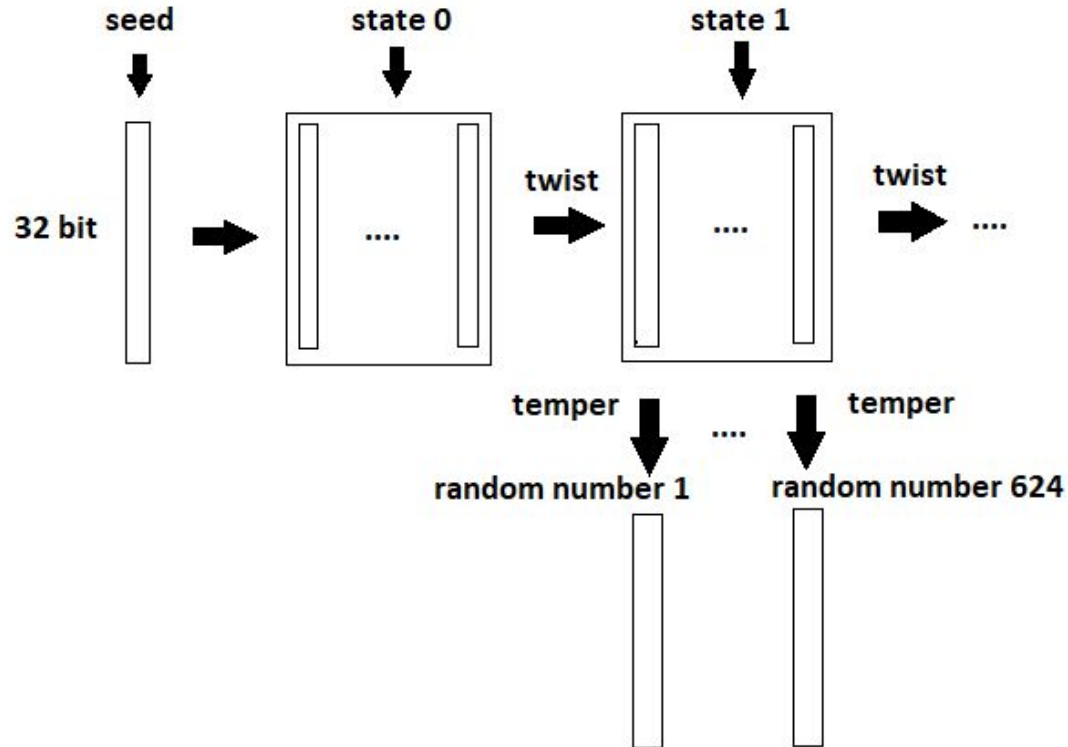


MERSENNE TWISTER (MT19937)

- Αναπτύχθηκε το 1997 από τους Matsumoto Makoto & Takuji Nishimura
- Πήρε το όνομα της από τη χρήση των Mersenne Primes
- Είναι η πρώτη γεννήτρια που μπόρεσε να παράγει τόσο υψηλής ποιότητας αριθμούς σε τόσο μικρό χρονικό διάστημα
- Βασίζεται στις γεννήτριες γραμμικών ισοδυναμιών
- Η MT19937 αποτελεί την προκαθορισμένη ψευδοτυχαία γεννήτρια σε πολλά λογισμικά συστήματα όπως Microsoft Excel, Maple , C compilers , Ruby , Python , Matlab , php και άλλα

$$x_{k+n} = x_{k+m} \oplus ((x_k^u \parallel x_{k+1}^l)A) \quad k = 0, 1, 2, \dots$$

MERSENNE TWISTER



SLOT MACHINE

- γλώσσα προγραμματισμού python 3.6 και περιβάλλον ανάπτυξης Pycharm
- βιβλιοθήκη Pygame v1.9.6
- γεννήτρια τυχαίων αριθμών MT19937



```

int[0..n-1] MT
int index = n+1
const int lower_mask = (1 << r) - 1
const int upper_mask = lowest w bits of (NOT lower_mask)

function init_seed(int seed) {
    index = n
    MT[0] = seed
    for i from 1 to (n - 1) {
        MT[i] = lowest w bits of (f * (MT[i-1] XOR (MT[i-1] >> (w-2))) + i)
    }
}

```

```

function extract_number() {
    if index >= n {
        twist()
    }

    int y = MT[index]
    y = y XOR ((y >> u) AND d)
    y = y XOR ((y << s) AND b)
    y = y XOR ((y << t) AND c)
    y = y XOR (y >> l)

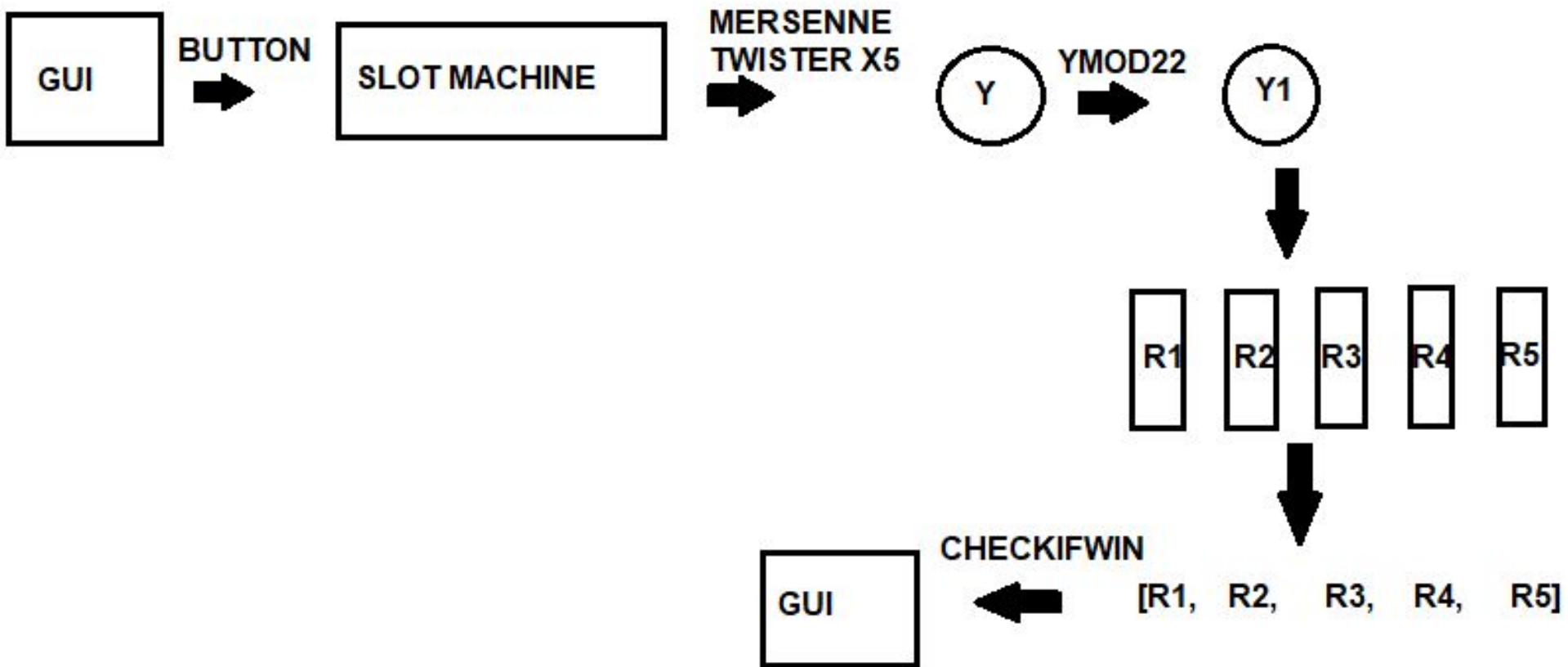
    index = index + 1
    return lowest w bits of (y)
}

```

```

function twist() {
    for i from 0 to (n-1) {
        int x = (MT[i] AND upper_mask)
                + (MT[(i+1) MOD n] AND lower_mask)
        int xA = x >> 1
        if (x MOD 2) != 0 {
            xA = xA XOR a
        }
        MT[i] = MT[(i + m) MOD n] XOR xA
    }
    index = 0
}

```







5	2500
4	500
3	250



5	500
4	200
3	75

WILD for all symbols except



5	150
4	60
3	20



5	100
4	50
3	15



5	75
4	25
3	10



5	60
4	25
3	10



5	50
4	15
3	5

Line wins must match on adjacent reels, beginning with leftmost reel.



CREDITS 500

LINES 5

BET - 5 +





ΕΥΧΑΡΙΣΤΩ ΠΟΛΥ ΓΙΑ ΤΟ ΧΡΟΝΟ ΣΑΣ