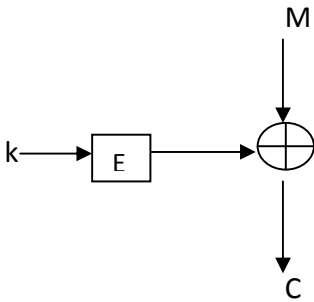


Network Security Notes (September 4 2009)

By Supreet Padhi

Stream Cipher



Properties of Expansion Function(E)-

- Look Random
- Long Output
- Given output shouldn't be able to inter the seed(k).
- No repeats
- Efficient
- Deterministic
- Can't predict the unknown portion of output from known portions.(next bit tests)

Example- Linear Congruential Generator

```
unsigned int state;
```

```
int E(void)
```

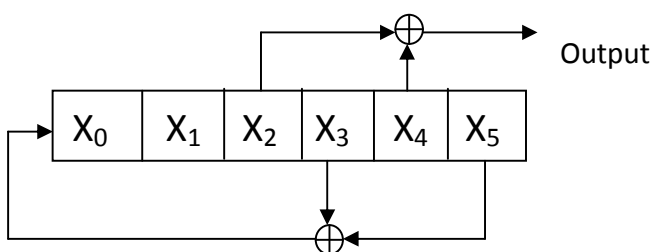
```
{
```

```
    state=322349*state+465749;
```

```
    retron state%2;
```

```
}
```

Linear Feedback Shift Register(LFSR)



("Broken by itself")

Blum-Blum-Stub(BBS)

Pick large primes p,q and $N=pq$.

Pick $X_0 \in \{2,3,\dots,N-1\}$

Let $X_i = X_{i-1}^2 \text{ mod } N$

Output_i = $X_i \text{ mod } 2$

Key = (X_0, N)

Breaking is equivalent to factoring N

Example – RC4 cipher used in WAP

Probability Distribution and Distinguishability

Definition- A probability distribution is a function that assigns a probability to each possible value in some set.

Ex- $D(0)=0.7$

$D(1)=0.3$

$X \leftarrow D$ (Pick an element X from distribution D)

Uniform Distribution

$$U_s(S) = \frac{1}{|S|}$$

Example-

$D = U_{\{0,1,2,3,4,5\}}$

$X \leftarrow D$

$X^2 \text{ mod } 6$

	$\frac{1}{6}$	$\frac{1}{6}$	$\frac{1}{6}$	$\frac{1}{6}$	$\frac{1}{6}$	$\frac{1}{6}$
X	0	1	2	3	4	5
	↓	↓	↓	↓	↓	↓
$X^2 \text{ mod } 6$	0	1	4	3		
	$\frac{1}{6}$	$\frac{1}{3}$	$\frac{1}{3}$	$\frac{1}{6}$		

Statistical Indistinguishability

Two distributions D and D' are ϵ - statistically indistinguishable if for all algorithm A

$$P_r[A(X) = 1 \mid X \leftarrow D] - P_r[A(X) = 1 \mid X \leftarrow D'] \leq \epsilon$$

Computational Indistinguishability

Definition- Distribution D and D' are (t, ϵ) computationally indistinguishable if for all algorithms running in time $\leq t$

$$\text{Adv } A \leq \epsilon$$

$$D \stackrel{t}{\sim}_{\epsilon} D'$$

Theorem- if $D_1 \stackrel{t}{\sim}_{\epsilon_1} D_2$ and $D_2 \stackrel{t}{\sim}_{\epsilon_2} D_3$ then $D_1 \stackrel{t}{\sim}_{\epsilon_1 + \epsilon_2} D_3$

Proof- Let A be any algorithm in time t then

$$|P_r[A(x)=1 \mid X \leftarrow D_1] - P_r[A(x)=1 \mid X \leftarrow D_3]|$$

$$= |P_r[A(x)=1 \mid X \leftarrow D_1] - P_r[A(x)=1 \mid X \leftarrow D_2] + P_r[A(x)=1 \mid X \leftarrow D_2] - P_r[A(x)=1 \mid X \leftarrow D_3]|$$

$$\leq |P_r[A(x)=1 \mid X \leftarrow D_1] - P_r[A(x)=1 \mid X \leftarrow D_2]| + |P_r[A(x)=1 \mid X \leftarrow D_2] - P_r[A(x)=1 \mid X \leftarrow D_3]|$$

$$\leq \epsilon_1 + \epsilon_2$$

Theorem – **Data Processing Inequality**

if $D \stackrel{t}{\sim}_{\epsilon} D'$ and f is any function computable in time t' then

$$f(D) \stackrel{t-t'}{\sim}_{\epsilon} f(D')$$

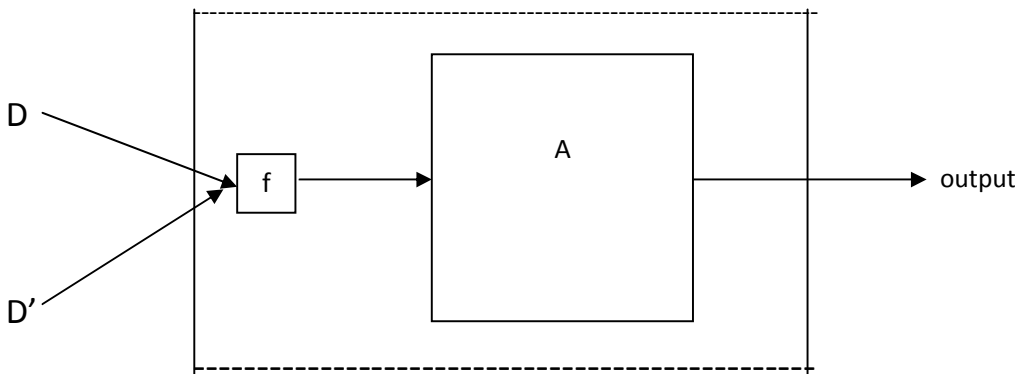
Note- $X \leftarrow D$

$f(D) \approx D_j$ then $f(X) \approx f^*D$

Proof(by contrapositive) :-

Suppose A running in time t-t' such that

$$\text{Adv}_{f(D), f(D')} A > \epsilon_1$$



$$1. P_r[A'(X)=1 \mid X \leftarrow D] = P_r[A(f(x))=1 \mid X \leftarrow D]$$

$$2. P_r[A'(X)=1 \mid X \leftarrow D'] = P_r[A(f(x))=1 \mid X \leftarrow D']$$

$$\text{So } \text{Adv}_{D, D'} A' = |P_r[A'(X)=1 \mid X \leftarrow D] - P_r[A'(X)=1 \mid X \leftarrow D']|$$

$$= |P_r[A(X)=1 \mid X \leftarrow f(D)] - P_r[A(X)=1 \mid X \leftarrow f(D')]|$$

=> $\text{Adv}_{D, D'} A' > \epsilon$ which is false. Hence proved.