

Network Security - CSE 508 - Fall 09

Faculty - Rob Johnson

Friday September 4, 2009

1 Stream Cipher

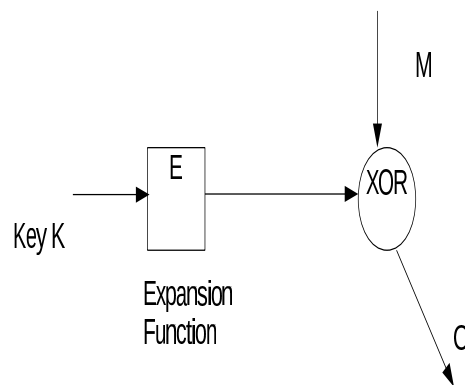


Figure 1: StreamCipher

2 Properties of expansion function E

- Should look random
- Should produce a long output
- Given the output, attacker should not be able to infer the seed
- No repeats
- The algorithm should be efficient
- The algorithm should be deterministic
- Should not be able to produce some unknown portions of the output from some known portions

3 Examples of Random Number generators

3.1 Linear Congruential Generator

```
unsigned int state;  
int E(void)  
{  
    state = 322349 * state + 45656749;  
    return state % 2;  
}
```

3.2 Linear Feedback Shift Register

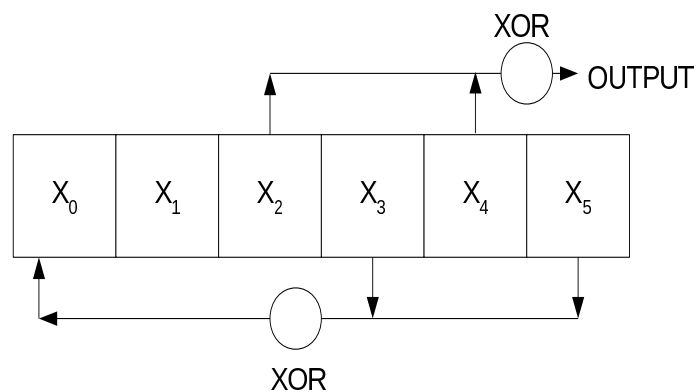


Figure 2: Linear Feedback Shift register

Though both Linear Congruential Generator and Linear Feedback Shift Register are used for random number generation, they are not completely safe and can be predicted.

3.3 Blum Blum Shub

Pick two large prime numbers p and q such that $N = pq$
Pick $X_0 \in \{2, 3, \dots, N - 1\}$
Let $X_i = X_{i-1}^2 \bmod N$
 $Output_i = X_i \bmod 2$
 $Key = (X_0, N)$

4 Probability Distribution and Distinguishability

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

Eg: If $D[0] = 0.7$ and $D[1] = 0.3$ then $X \leftarrow D$ would mean to pick an element from the Set $\{0, 1\}$ according to the distribution D .

Uniform Distribution: $U_S(s) = \frac{1}{|S|}$

Example: $D = U_{\{0,1,2,3,4,5\}}$ and $X \leftarrow D$ then $X^2 \bmod 6$ is equal to

	1/6	2/6	3/6	4/6	5/6	6/6
X	0	1	2	3	4	5
X^2	0	1	4	3	4	1

Hence, $Pr(X^2 = 0) = 1/6$

$Pr(X^2 = 1) = 1/3$

$Pr(X^2 = 3) = 1/3$

$Pr(X^2 = 4) = 1/6$

Which shows that, we can perform computations on any distribution and the resultant distribution might vary from the actual random variable.

5 Statistical Indistinguishability

Definition: Two distributions D and D' are ϵ -statistically indistinguishable for all Algorithms A if

$$\text{Adv } A = |Pr[A(X) = 1 | X \leftarrow D] - Pr[A(X) = 1 | X \leftarrow D']| \leq \epsilon$$

$A()$ is the adversary algorithm which has infinite time and knowledge

Distributions D and D' are t, ϵ -computationally indistinguishably if for all algorithms A running in time $\leq t$, $\text{Adv } A \leq \epsilon$

6 Theorem

- If $D_1 \sim_{\epsilon_1, t} D_2$ and $D_2 \sim_{\epsilon_2, t} D_3$ then $D_1 \sim_{\epsilon_1 + \epsilon_2, t} D_3$

Let A be any algorithm running in time t , then,

$$\begin{aligned} & |Pr[A(X) = 1 | X \leftarrow D_1] - Pr[A(X) = 1 | X \leftarrow D_3]| \\ & |Pr[A(X) = 1 | X \leftarrow D_1] - Pr[A(X) = 1 | X \leftarrow D_2]| + Pr[A(X) = 1 | X \leftarrow D_2] - Pr[A(X) = 1 | X \leftarrow D_3]| \\ & \leq |Pr[A(X) = 1 | X \leftarrow D_1] - Pr[A(X) = 1 | X \leftarrow D_2]| + |Pr[A(X) = 1 | X \leftarrow D_2] - Pr[A(X) = 1 | X \leftarrow D_3]| \\ & \leq \epsilon_1 + \epsilon_2 \\ & \text{Q.E.D.} \end{aligned}$$

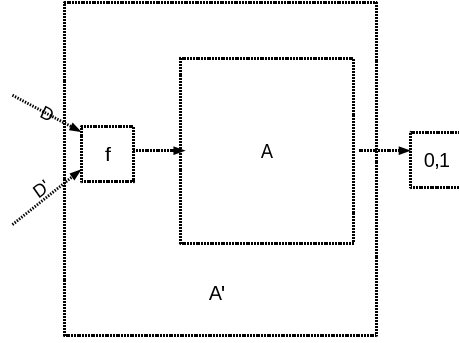


Figure showing $A'(x) = A(f(x))$

Figure 3: Data Processing Inequality

7 Theorem: Data Processing Inequality

- If $D \sim_{t,\epsilon} D'$ and f is any function computable in time t' , then $f(D) \sim_{t-t',\epsilon} f(D')$

Modified adversary algorithm A' is a combination of adversary algorithm A and function $f()$, such that $A'(x) = A(f(x))$

Proof (By contrapositive): Suppose $\exists A$ running in time $t - t'$ such that

$Adv_{f(D),f(D')} A > \epsilon$, then,

$$Pr[A'(X) = 1 | X \leftarrow D] = Pr[Af((X)) = 1 | X \leftarrow D] = Pr[Af((X)) = 1 | X \leftarrow f(D)]$$

$$Pr[A'(X) = 1 | X \leftarrow D'] = Pr[Af((X)) = 1 | X \leftarrow D'] = Pr[Af((X)) = 1 | X \leftarrow f(D')]$$

So $Adv_{D,D'} A' = |Pr[A'(X) = 1 | X \leftarrow D] - Pr[A'(X) = 1 | X \leftarrow D']|$

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

$$= Adv A > \epsilon$$