

Network Security, Lecture Notes, Class 2

September 4, 2009

1 Stream Ciphers

- Uses symmetric keys for encryption and decryption.
- One-time pad is one of the best-known stream ciphers.

1.1 Properties of Expansion Function

The Expansion function:

- Should Look Random
- Output should be long
- Given the output, we should not be able to infer the seed
- No repetitions
- Not computationally too complicated (Efficiency)
- Deterministic
- We should not be able to predict unknown portions of the output from some of the known portions. This is known as the Next-bit test i.e. given the present bit, we should not be able to predict the next bit.

1.2 Pseudo Random Number Generators

1. Linear Congruential Generator: This is a very simple and efficient LCG. The equation for an LCG is as follows:

$$X_n = a * X_{n-1} + m$$

where: X_n is the nth number in the sequence, X_{n-1} is the previous number, a is the multiplier, b is the increment, m is the modulus, and X_0 .

```
unsigned int state;
```

```
int E(void)
```

```
{  
state = 322349 * state + 45656749;  
return state % 2;  
}
```

2. Linear Feedback Shift Register: An LFSR consists of a shift register and a feedback function. The shift register is a sequence of bits. Each time a bit is needed, all the bits are shifted one bit to the right.

An example of an LFSR is:

$$\begin{array}{cccccc} X_0 & X_1 & X_2 & X_3 & X_4 & X_5 \\ \text{Output} & : & X_2 \oplus X_4 & & & \\ \text{Feedback} & : & X_3 + X_5 \rightarrow X_0 & & & \end{array}$$

3. Blum Blum Shub (BBS):

- Pick large primes p & q such that $N = p \cdot q$;
- Pick $X_0 \in \{2, 3, \dots, N-1\}$
- Let $X_i = X_{i-1}^2 \bmod N$
- $\text{Output}_i = X_i \bmod 2$
- (X_0, N) forms the key k .

Breaking is equivalent to factoring N .

2 Probability Distribution and Distinguishability

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

Eg: $D(0) = 0.7$ $D(1) = 0.3$

$X \leftarrow D$.

$D(X)$ denotes the probability of drawing an element X from the set D .

For a finite set S , the uniform distribution $u_S(s) = 1/|S|$. u_l on an l -bit string indicates uniform distribution.

2.1 Statistical and Computational Indistinguishability

- Compare 2 Distributions.
- Two distributions D and D' are ϵ -statistically indistinguishable if for all algorithm A , then:

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

Definition: Distributions D & D' are t, ϵ -computationally indistinguishable if for all algorithms A running in time $\leq t$,

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

Notation: $D \tilde{t}, \epsilon D'$ denotes indistinguishability i.e they are similar. **Theorem:**
If $D_1 \tilde{t}, \epsilon D_2$ and $D_2 \tilde{t}, \epsilon D_3$ then, $D_1 \tilde{t}, \epsilon_1 + \epsilon_2 D_3$ Proof: Let A be any algorithm running in time t . Then,

$$\begin{aligned}
& |Pr[A(X) = 1/X \leftarrow D_1] - Pr[A(X) = 1/X \leftarrow D_3]| \\
&= |Pr[A(X) = 1/X \leftarrow D_1] - Pr[A(X) = 1/X \leftarrow D_2]| + Pr[A(X) = 1/X \leftarrow D_2] - Pr[A(X) = 1/X \leftarrow D_3]| \\
&\leq |Pr[A(X) = 1/X \leftarrow D_1] - Pr[A(X) = 1/X \leftarrow D_2]| + Pr[A(X) = 1/X \leftarrow D_2] - Pr[A(X) = 1/X \leftarrow D_3]| \\
&\leq \epsilon \text{ If } D \text{ and } D' \text{ are statistically indistinguishable, then they are computationally indistinguishable.}
\end{aligned}$$

2.2 Data Processing Inequality

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

Proof: (Proof by contrapositive)

Suppose $\exists A$, running in time $t-t'$ such that $Adv_{f(D), f(D')} A > \epsilon$

1. $Pr[A'(X) = 1/X \leftarrow D] = Pr[A(f(X)) = 1/X \leftarrow D] = Pr[A(X) = 1/X \leftarrow f(D)]$

2. $Pr[A'(X) = 1/X \leftarrow D'] = Pr[A(f(X)) = 1/X \leftarrow D']$

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

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

Hence, if $f(D) \tilde{t} - t', \epsilon f(D')$ then, $D \tilde{t}, \epsilon D'$