

Network Security

Sumeet P Dash

September 4, 2009

Stream Cipher

1. Symmetric key cipher.
2. Uses a pseudorandom bit stream as key.
3. Approximates the action of the most secure One Time Pad(OTP).
4. Uses an expansion function to generate a pseudorandom keystream from a small and manageable key.
5. Because the key stream is not purely random as in the OTP, the scheme is less secure than the OTP.

Desirable Properties of The Expansion Function

1. Output should be as random as possible.
2. Output should be long enough to encode the plaintext at hand.
3. Given a ciphertext, one shouldn't be able to infer the seed.
4. Should be computationally efficient.
5. Should be deterministic.
6. If portions of the output are known, then the missing section shouldn't be predictable based on this knowledge. (Next-bit Tests)

The Linear Congruential Generator

The Linear Congruential Generator serves as an example of an expansion function which can be used in the context of a stream cipher and is easy to understand and efficient.

However it is not secure when used by itself.

A Sample Implementation

```
unsigned int state;

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

Linear Feedback Shift Register

A Linear Feedback Shift Register(LFSR) can also be deployed as an expansion function to be used with stream ciphers.

$$\begin{aligned} & [X_0][X_1][X_1][X_3][X_4][X_5] \\ & X_5 \oplus X_3 \rightarrow X_0 \\ & X_2 \oplus X_4 \rightarrow \text{Output} \end{aligned}$$

It is easily broken when used by itself.

Blum Blum Shub

Blum Blum Shub(BBS) is another example of an expansion function.

It is of the following form:

$$\begin{aligned} & \text{Pick } X_0 \in \{2, 3, N - 1\} \\ & X_i = X_i^2 \text{ mod } N \end{aligned}$$

where $N = pq$ is the product of two large primes p and q .

$$\begin{aligned} & \text{Output} = X_i \text{ mod } 2 \\ & \text{Key} = (X_0, N) \end{aligned}$$

Breaking is as hard as factoring N .

Probability Distribution and Distinguishability

A probability distribution is a function that assigns a probability to each value present in a given set.

$$X \leftarrow D$$

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

Statistical Indistinguishability

Two distributions D and D' are ϵ -statistically indistinguishable if \forall algorithm A

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

where $A(X) = 1$ if A believes that X was drawn from D (as opposed to D').

Computational Indistinguishability

Two distributions D and D' are t, ϵ -computationally indistinguishable if \forall algorithm A running in time $\leq t$

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

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

In the same token two statistically indistinguishable distributions can be expressed as: $D \stackrel{\infty}{\sim}_{\epsilon} D'$

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 running in time t . Then

$$\begin{aligned} & | \Pr[A(X) = 1 | X \leftarrow D_1] - \Pr[A(X) = 1 | X \leftarrow D_3] | \\ &= | \Pr[A(X) = 1 | X \leftarrow D_1] - \Pr[A(X) = 1 | X \leftarrow D_2] + \Pr[A(X) = 1 | X \leftarrow D_2] - \Pr[A(X) = 1 | X \leftarrow D_3] | \\ &\leq | \Pr[A(X) = 1 | X \leftarrow D_1] - \Pr[A(X) = 1 | X \leftarrow D_2] | + | \Pr[A(X) = 1 | X \leftarrow D_2] - \Pr[A(X) = 1 | X \leftarrow D_3] | \leq \epsilon_1 + \epsilon_2 \quad \square \end{aligned}$$

Data Processing Inequality

If $D \stackrel{t}{\sim}_{\epsilon_1} D'$ and f is any function computable in time t' then $f(D) \stackrel{t-t'}{\sim}_{\epsilon_1} f(D')$.

proof (By Contrapositive)

Suppose $\exists A$ running in time $t - t'$ s.t. $\text{Adv}_{f(D)-f(D')} A > \epsilon$

$$\begin{array}{l} D \rightarrow \\ D' \rightarrow \end{array} \left[[f] \rightarrow [A] \right]^{A'} \rightarrow \text{Output}$$

Now,

$$\begin{aligned} \text{Adv}_{D-D'} A' &= | \Pr[A'(X) = 1 | X \leftarrow D] - \Pr[A'(X) = 1 | X \leftarrow D'] | \\ &= | \Pr[A'(f(X)) = 1 | X \leftarrow D] - \Pr[A'(f(X)) = 1 | X \leftarrow D'] | \\ &= | \Pr[A(X) = 1 | X \leftarrow f(D)] - \Pr[A(X) = 1 | X \leftarrow f(D')] | \\ &= \text{Adv}_{f(D)-f(D')} A \end{aligned}$$

$$\Rightarrow \text{Adv}_{D-D'} A' > \epsilon$$

which is false. Hence proved.