CS 346 Class Notes

Mark Lindberg

Mar 21, 2016

Last Time:
HW stuff.
4.29:

$$\begin{bmatrix} k_{1,1} & k_{1,2} & k_{1,3} & \cdots & 1,n \\ k_{2,1} & k_{1,1} & k_{1,2} & \cdots & 2,n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ k_{\ell,1} & k_{\ell-1,2} & k_{\ell-2,3} & \cdots & \ell-n+1,1 \end{bmatrix}$$

Somehow it's diagonal filled, so defining the first column and row define the entire matrix. $k_{\ell-n+1,1} = k_{\max(1,\ell-n+1),max(1,n-\ell+1)}$.
This Time:
Whirlwind tour of chapter 6.
Practical constructions of symmetric key primitives.
6.1. Stream Ciphers.
These are analogous to PRGs.
6.1.1 Linear Feedback Shift Register
There are n bits of state. For each bit of output, shift each of the bits of the state, s_0 shifts off as our next random bit, and s_{n-1} will be replaced with the $\oplus$ of some subset of the remaining bits. This can be implemented extremely efficiently in hardware.

Seeing $2n$ output bits is enough to determine the initial state $s_0, s_n - 1$ *and* the subset of bits which are $\oplus$ed together to form each successive s_{n-1} value.
This is not a good proxy for a PRG at all.
6.1.2 Adding Nonlinearity

1. Nonlinear feedback function.

2. Output bit is a non-linear function of the state.

3. "Nonlinear combination generators".

Trinium: Developed in 2008.

Based on 3 LFSRs.

93 bit LFSR A, 84 bit LFSR B, and 111 bit LFSR C, for a total of 288 bits.

There's a really complicated diagram of how this actually works.

1152 pre-computer iterations is the magic number. :P

Older: RC4 - No longer recommended for use.

Designed for fast software implementation.

It uses byte operations and array indexing.

It is initialized with (S, i, j), where S is a 256-byte array, and i and j are indices in the array.

The key is 16 bytes (in our example).

Again, there is a weird diagram for how it is initialized.

Wikipedia explanation.

6.2 Block Ciphers. (Practical implementation of strong PRPs.)

Fixed key length, and input length = output length (block length).

DES: Block length is 64 bits. Key length is 56 bits.

Triple DES: Key length is 112 bits.

Substitution-Permutation Networks:

Based on Shannon's "confusion-diffusion paradigm"

Block length: 128 bits.

There are $2^{128}!$ permutations. HOLY. That number has 10^{40} DIGITS. If we index from 0, we need $\log_2(2^{128}!)$ bits, which is $> 2^128$. Yeah.

There's another diagram.

Substitution Permutation Networks: SPN.

Use fixed permutations for the f's. Where is the key used?

1. Key mixing - xor input with a round subkey.
2. Substitution - confusion via fixed permutations.
3. Permutation - Diffusion.