Notes for class of 18.8

Note Title 2020-08-17

Practical Vernam cipher: (Stream cipher) : A is a field

Algorithm:
1. Exchang key K
2. Choose a random IV
3. Initial state $x(0) = (K, IV)$
   Generate sequence of states $x(k+1) = F(x(k))$
4. Generate output stream
   $w(k) = f(x(k))$ in A
5. Encrypt: $c(k) = p(k) + w(k)$

Decryption by same algorithm: $p(k) = c(k) - w(k)$

As a TOWF: $\{c(k)\} = E(K, \{p(k)\})$

1. OWF from $\{p(k)\}$ to $\{c(k)\}$ given K.
2. Easy to invert from $\{c(k)\}$ to $\{p(k)\}$ given K.
3. Given both $\{p(k)\}$ and $\{c(k)\}$ (alt. given $w(k)$) difficult to find K.

- Since Encryption is like a Vernam cipher / OTP property 1 is assured by randomness of $\{w(k)\}$ for any IV.

< Output stream should be indistinguishable from a random stream of alphabets >

- Since the algorithm to generate output stream from IV is deterministic the output sequence is pseudo-random (PR) stream cipher is thus a PRG.