Stream Ciphers

CSCI283/172 Fall 2008

GW

Example: one-time pad

$P = C = Z_{2^n}$

$d_K = e_K(x_1, x_2, \ldots x_n) = (x_1+K_1, x_2+K_2, \ldots x_n+K_n)$ *mod 2*

Problems?

One-time pad is best

- But key too long to be practical
- Can we use a pseudo-random key then, which would be generated from a short truly random string?