Lecture 3 (incomplete)

Lecture Notes: 2.5, 4.1 – 4.5

# Old vs New SC

## Old

* Only the key was used to create the keystream.
* Need a new key for every message.

## New

* Add a diversifier
* SC (K, D1) 🡪 Z1 = …  
   🡪 C1 = Z1 + M1
* Diversifier is sent with the Ciphertext to the other party.
* A diversifier can be a date, message sequence number, random value, …

# How not to build a stream cipher

* S(i) = Mt(K + D(i)) = MtK + MtD(i)
* M = Matrix
* It is important that Matrix M is linear
* Linear cryptographic schemes are not secure