Stream ciphers: stream encryption and LFSRs

# Modular arithmetic

* **Z** = Set of integers
* Z/2Z = Z mod 2
* Z/26Z = Z mod 26

# One time pad

* XOR operation using the message **M** and key **K** into cipher **C**
* One time pad is not desirable for daily operations, it works for military operations
* Stream cipher converts a short key **K** into long keystream **Z**
* **M** bitwise-+ **Z** = **C**

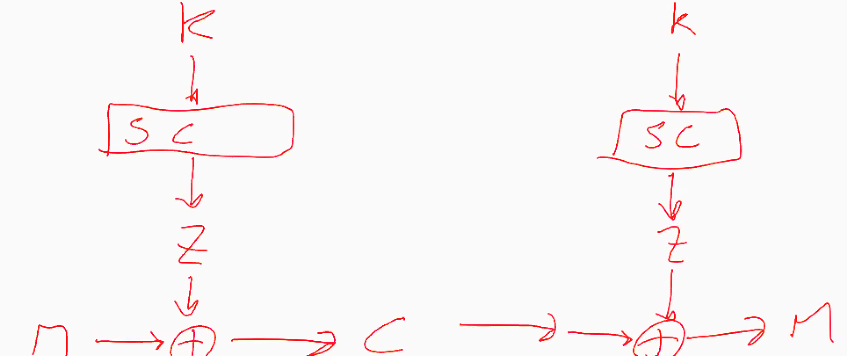


Figure 1 Encryption -> Decryption

# Vigienère cipher

* Repeat the shot Z/Z26 key (e.g. LEMON)
* Compact and efficient.
* Easy to break, just try all n letter words for n being the length of the key.
  + This ends in 26^5 attempts to break the encryption.
  + Only if the attacker knows the keys length
* Because of repeating, you can break the encryption easier because of repetition, as there is a case study for frequency of letters in words.
* Using part of the plain text and the cipher text, you can get part of the key, which is a repeating word.

# Linear feedback shift registers

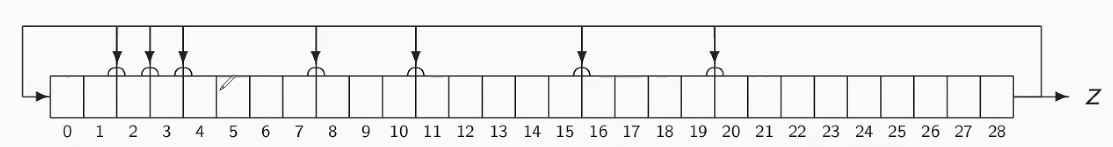


Figure 2 Galois LFSR

* Goal: Efficiently generate a non-repeating sequence **Z**
* Update: shift every bit to the right
* For some positions (feedback taps) Si+1 🡨 Si + S28
  + E.g. S11 🡨 S1 + S28
* Cycle length is 2­n – 1 if chosen properly.

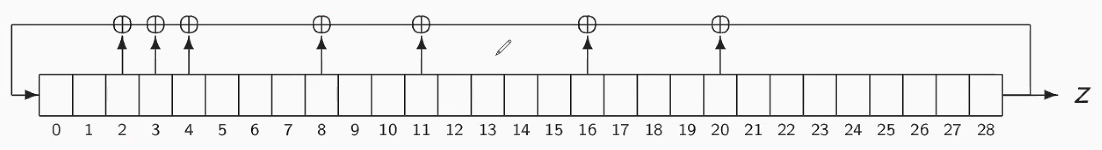


Figure 3 Fibonacci LFSR

* One can prove that for every Fibonacci LFSR there is a Galois LFSR generating the same sequence Z
* Each has their own advantages
  + Galois is more parallel, Fibonacci is more serial
  + Galois reveals finite field operations, Fibonacci recursion in sequence
* LFSR is very easy to implement, just a shift and some XORs
* LFSR algorithm is defined by the taps and the length
* Kerckhoffs principle: security should be based on secrecy of **K**, not on the secrecy of the algorithm

# Attacks on stream ciphers

* TODO watch again
* Setting: Adversary can obtain n subsequent bits of keystream zt­.   
  Using a known plaintext attack. ( Z = M XOR C )
* A function f is linear (over Z/2Z) if f(x+y) = f(x) + f(y) if f1 and f2 are linear.