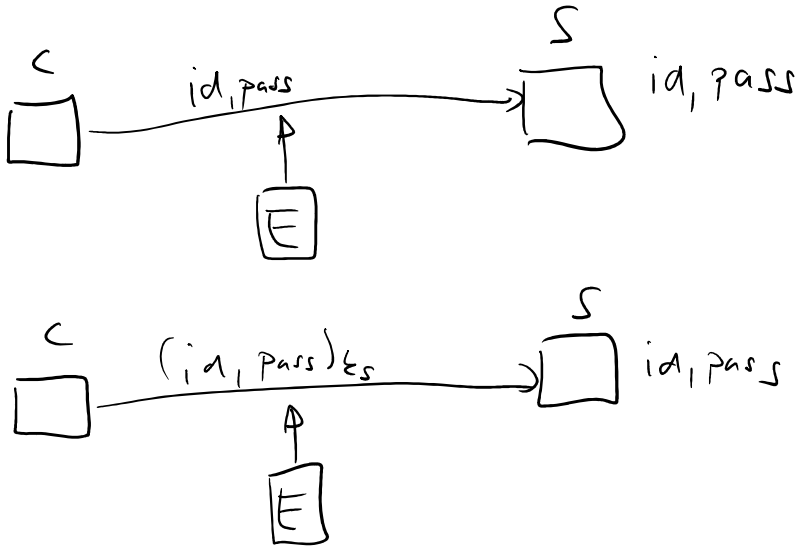
Tutorial XIII group 2

12 December 2019 16:03

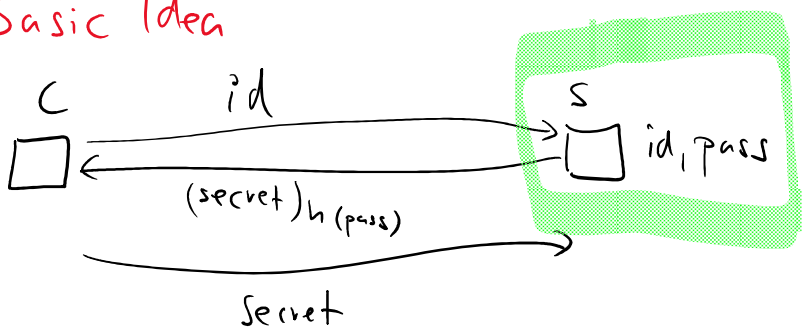
Inentification - Kerberos protocol

Linear feedback shift registers (LFSR)

Inaenthication

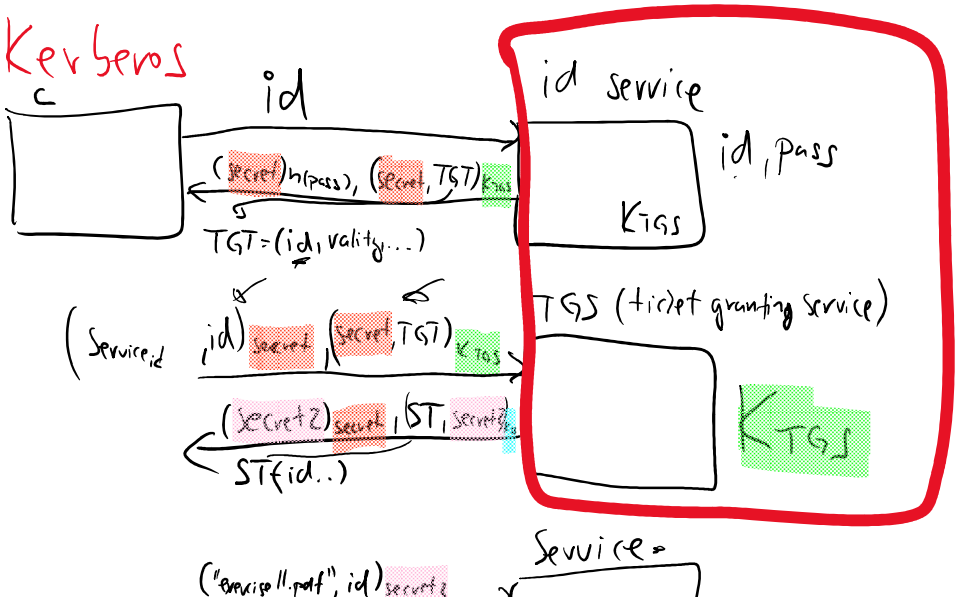


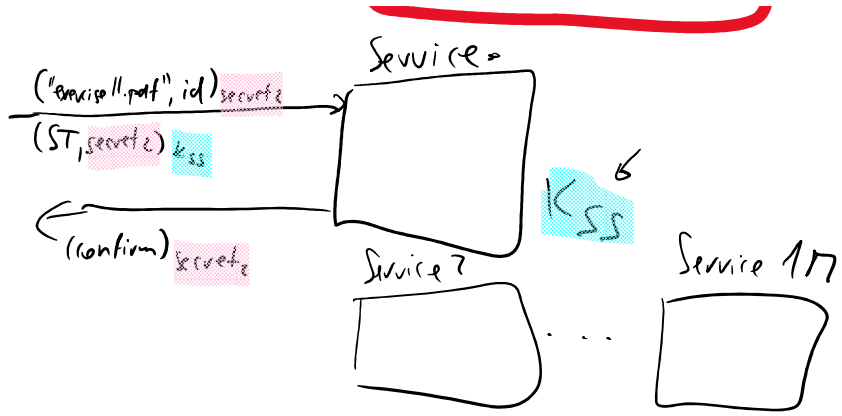
Basic Idea



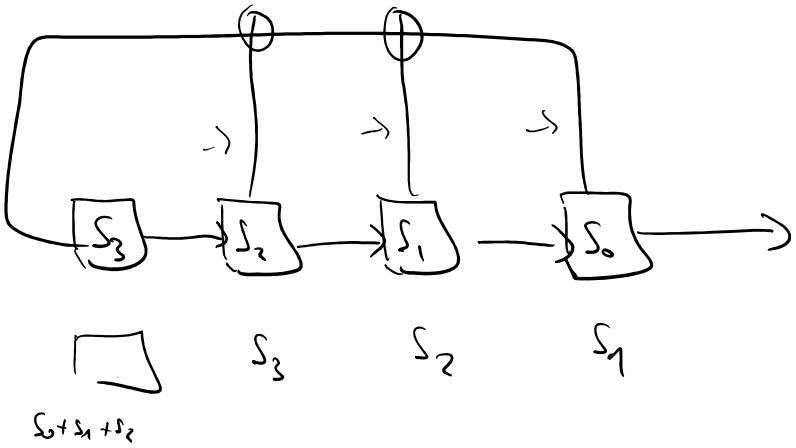
h(pass) ~ h(password, salt)

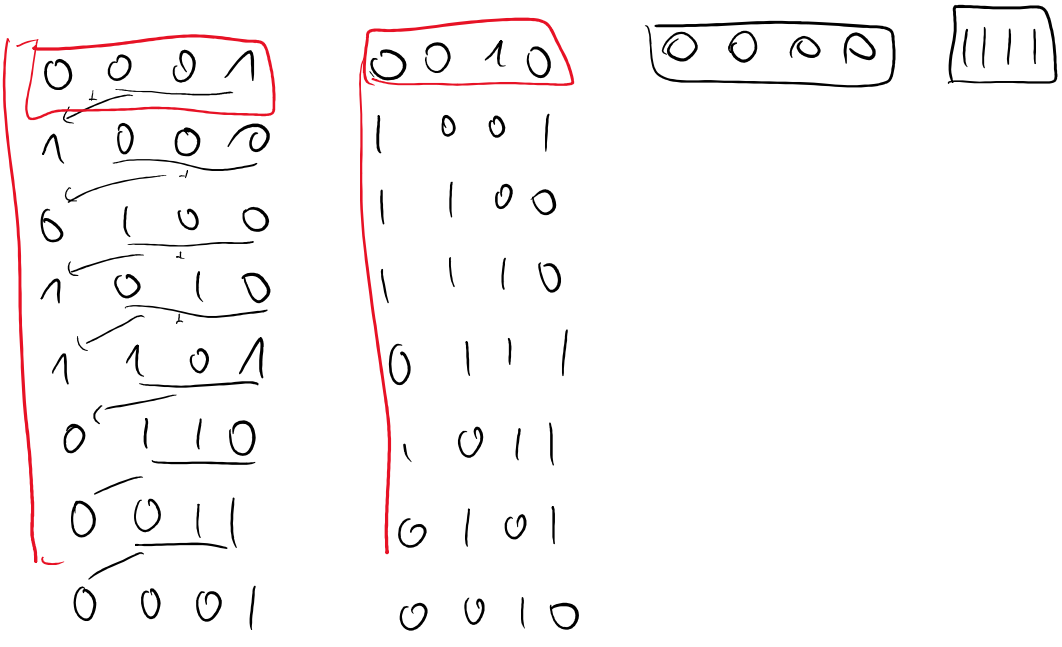
Kerberos

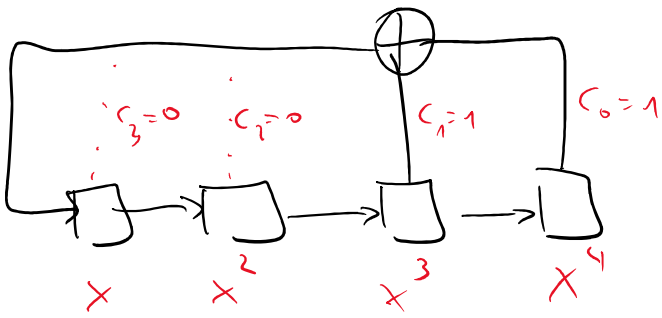




Linear-feedback shift registers

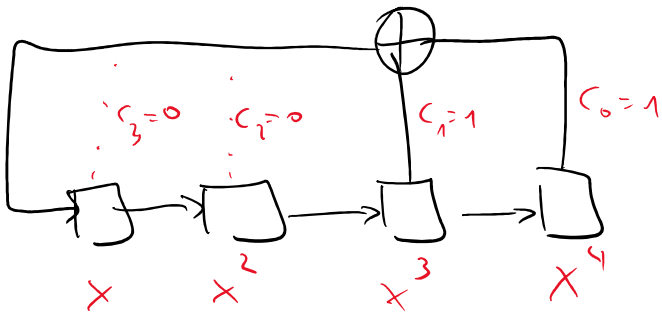




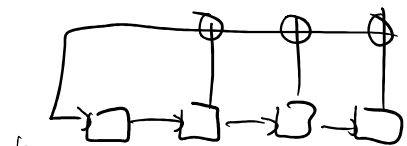


0 0 0 1
1 0 0 0
0 1 0 0
0 0 1 0
1 0 0 1
1 1 0 0
0 1 1 0
1 0 1 1
0 1 0 1
1 0 1 0
1 1 0 1
1 1 1 0
1 1 1 1
0 1 1 1
0 0 1 1
0 0 0 1

Charcteristic polynomials



$$f(x) = x^4 + x^3 + 1$$



$$f(x) = x^4 + x^3 + x^2 + 1$$

$$f(x) = \sum_{i=1}^{n} c_{n-i} x^i + 1$$

Thm

LFSR of size n has a period of size $2^n - 1$ iff $f(x)$ is a primitive polynomial in $\mathbb{Z}_2$.

irreducible polynomial: cannot be written as a product of other two polynomials

thm - each irreducible polynomial $f(x)$ divides a polynomial $x^k - 1$ for some k $\left(\deg(f(x)) < k \leq 2^{\deg(f(x))}\right)$

primitive polynomial is irreducible and smallest k for which it divides $x^k - 1$ is $k = 2^{\deg(f(x))}$

---

seed -> LFSR -> $2^{seed} - 1$ -> key in OTP

Suspectible to a known plaintext attack.

=> attacker knows a pair of plaintext and corresponding ciphertext

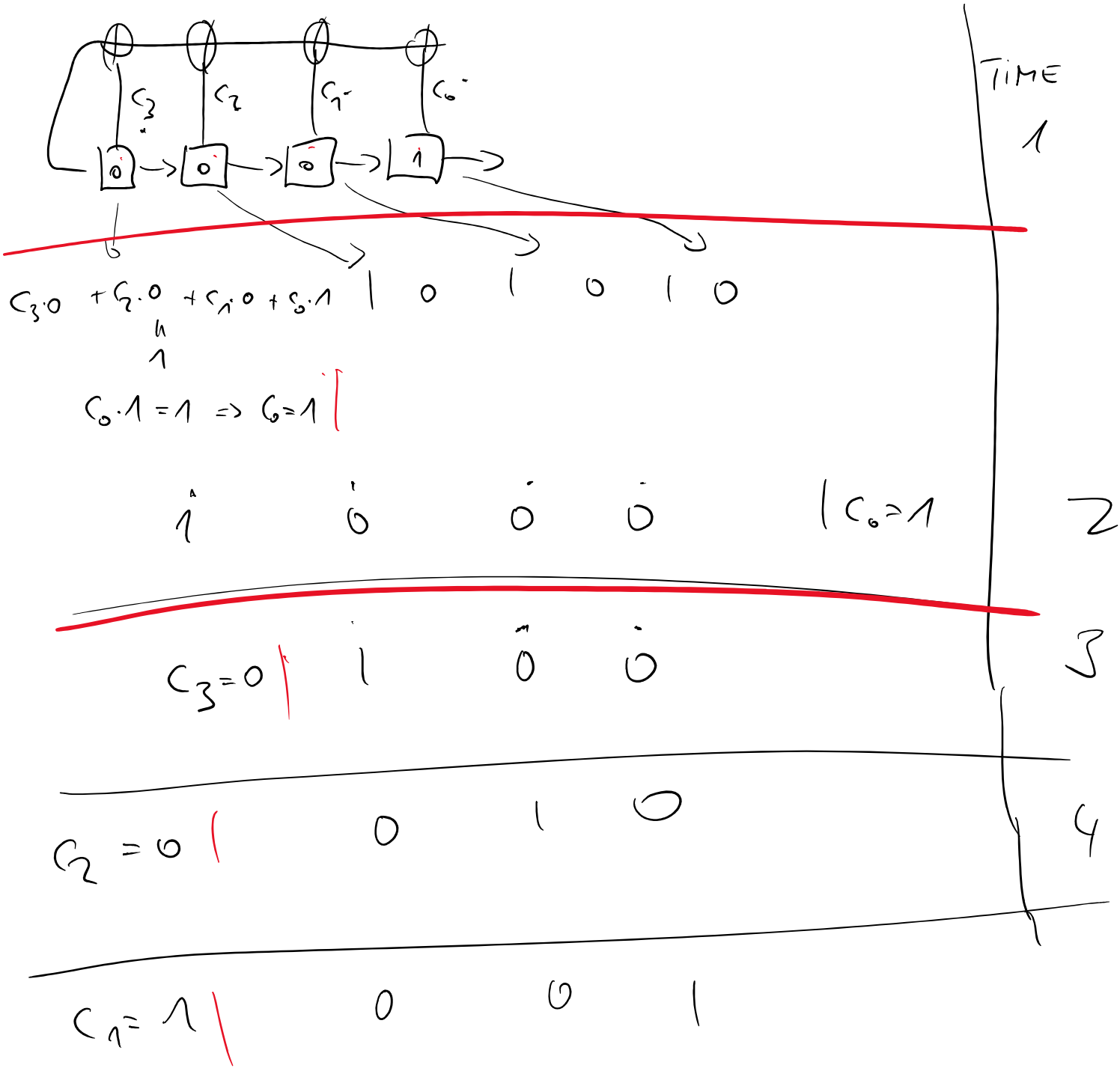
=> to break OTP, attacker requires $2n$ bits only

=> the attacker knows $2n$ bits of the key

1000 1001 are first 8 bits of LFSR of size 4

initial state

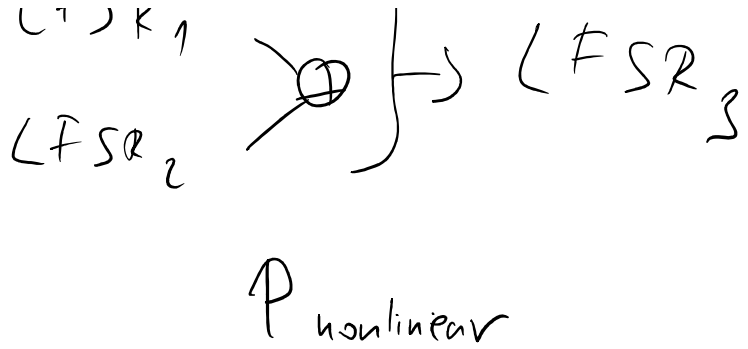
0 0 0 1



Now we know c_0, c_1, c_2 and c_3 as well as initial vector

=> we can generate the whole key and decrypt the ciphertext.

LFSR$_1$ $\not\mapsto$ LFSR$_2$


LFSR1
LFSR2
LFSR3
P nonlinear