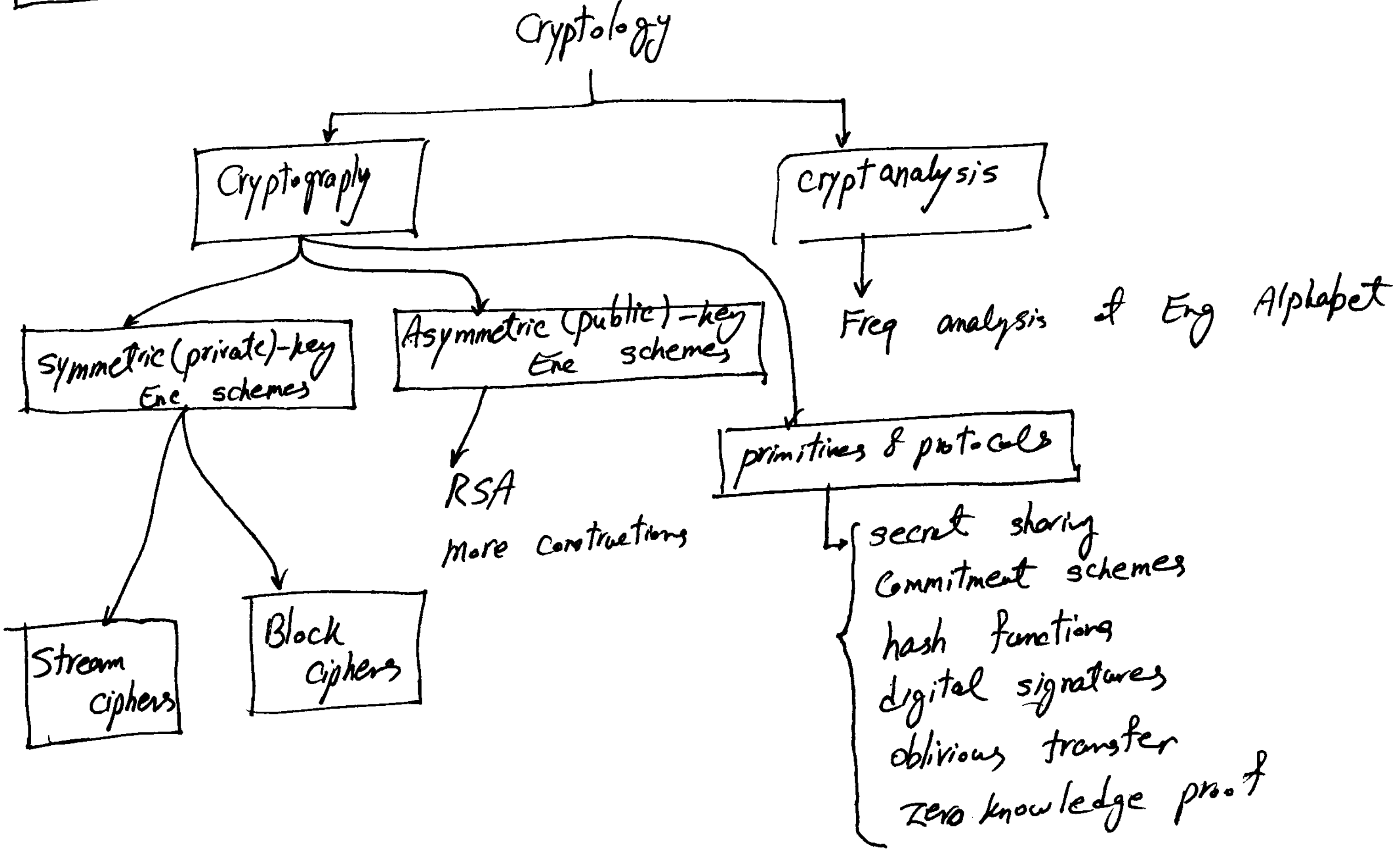
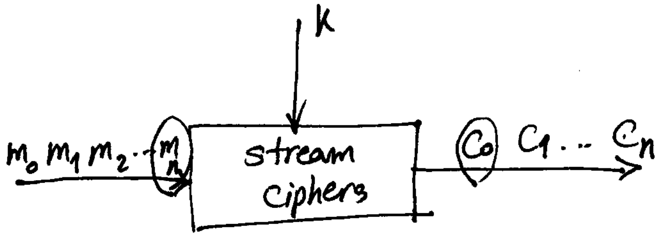
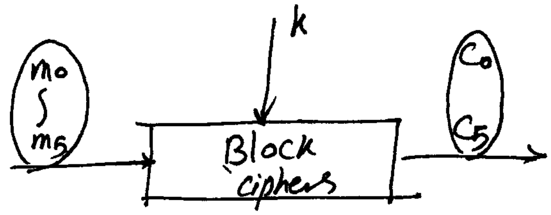
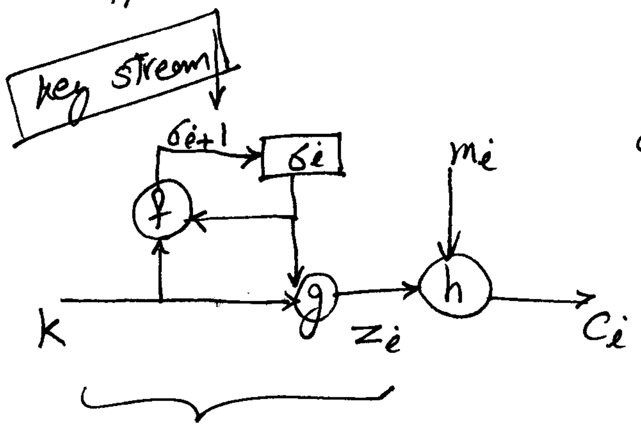






- Enc bits individually
- small & fast
- App: cell phones

- Enc Block of bits
- App: Internet protocols

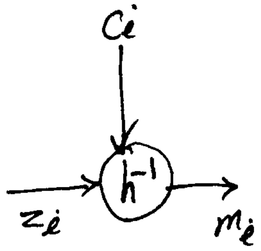


$\sigma_{i+1} = f(\sigma_i, k)$

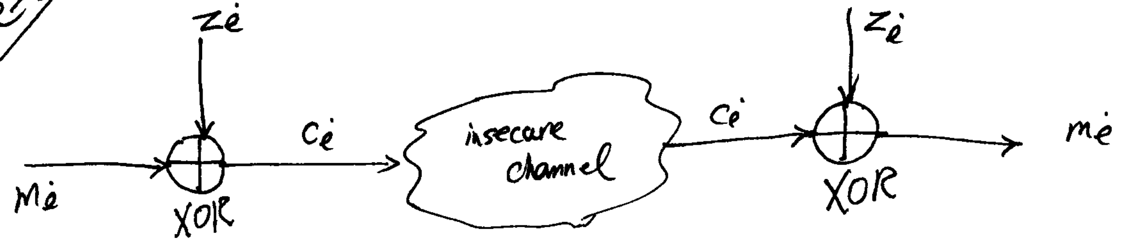
$z_i = g(\sigma_i, k)$

$c_i = h(z_i, m_i)$

$m_i = h^{-1}(z_i, c_i)$



Example-1



		XOR
0	0	0
0	1	1
1	0	1
1	1	0

addition (mod 2)

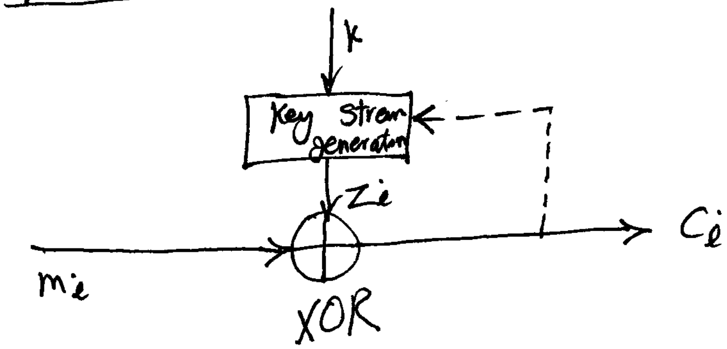
Enc & Dec functions are the same

m_i	z_i	c_i	c_i	z_i	m_i
0	0	0	0	0	0
0	1	1	1	1	0
1	0	1	0	1	1
1	1	0	1	0	1

$$Enc_{z_i}(m_i) = m_i + z_i \pmod 2$$

$$Dec_{z_i}(c_i) = c_i + z_i \pmod 2$$

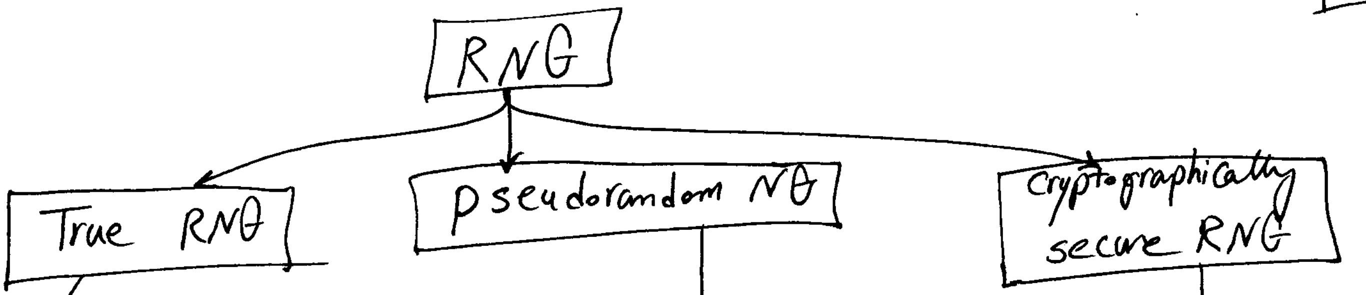
Asynchronous stream ciphers



key stream depends on the ciphertext

Synchronous stream ciphers

key stream depends only on the key



physical Rondom process

- dice rolling
- coin flipping
- semiconducter noise
- mouse movemet
- radioactive decay

$pr(z_i=0) = pr(z_i=1) = 1/2$

50%

	H	T
fair coin	1/2	1/2
baised coin	3/4	1/4

$f_{i+1}(n) = A f_i(n) + B \pmod P$

Initial seed values

$$\begin{cases} f_0 = seed \\ f_{i+1} = Af_i + B \pmod P \\ \text{size of } A, B, f_i \text{ is } \underline{100 \text{ bits}} \end{cases}$$

300 bits of output → f_1, f_2, f_3

$$\begin{cases} f_2 = Af_1 + B \pmod P \\ f_3 = Af_2 + B \pmod P \end{cases}$$

2 unknows & 2 equ

A, B

output must be unpredictable

↓

given "n" consecutive bits of the output z_i, the following output bits z_{i+1} cannot be predicted

Note: one-way functions

$$\begin{tikzcd} x \arrow[r, bend left, "easy"] & y = f(x) \arrow[l, bend left, dashed, "hard"] \end{tikzcd}$$

$f(x) = 3^x \pmod{17}$

$D_f = \{1 \sim 16\}$

$x \rightarrow$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$y \rightarrow$	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	1

$x = 11 \longrightarrow 3^{11} \pmod{17} \Rightarrow y = 7$

$y = 7 \longrightarrow x = ?$

One-Time pad (OTP)

$e_{k_i}(m_i) = m_i \oplus k_i$ ⟶ XOR function

$d_{k_i}(c_i) = c_i \oplus k_i$

$\downarrow$

$c_0 = m_0 \oplus k_0$

$c_1 = m_1 \oplus k_1$

$c_2 = m_2 \oplus k_2$

$\vdots$

c_0, c_1, c_2 are know to the adversary

↓

2 unknows & 1 equ for each bit

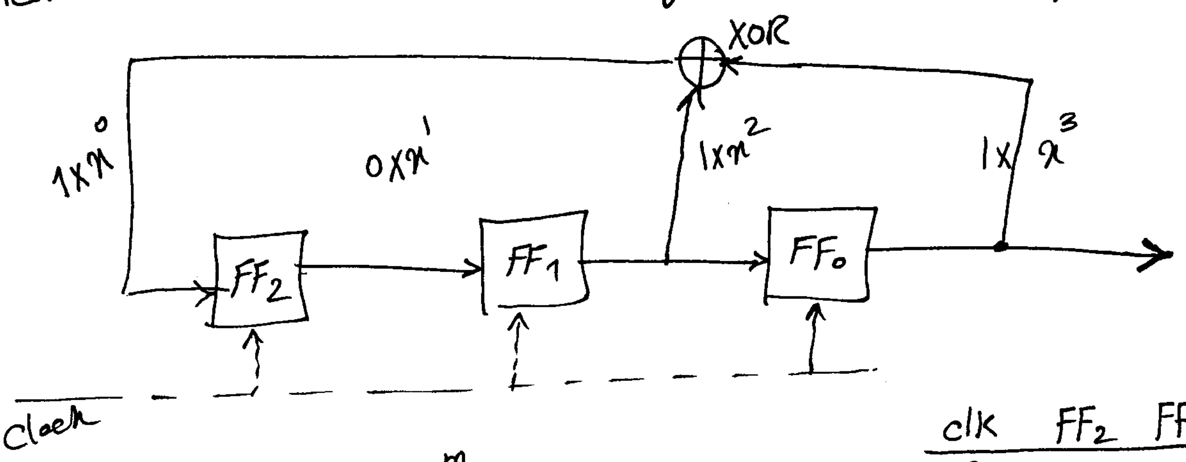
↓

secure

negative points {
- size of the key ⟶ $\underset{\text{size}}{\text{message}} = \underset{\text{size}}{\text{key}}$ X
- key must be used only once ...

Linear Feedback shift Registers (LFSR)

Example-2



$m = 3 \longrightarrow 2^m - 1 = 7$

poly $\longrightarrow f(x) = 1 + x^2 + x^3$

	clk	FF_2	FF_1	FF_0
Ini	0	1	0	0
	1	0	1	0
	2	1	0	1
	3	1	1	0
	4	1	1	1
	5	0	1	1
	6	0	0	1
	7	1	0	0
	8	0	1	0

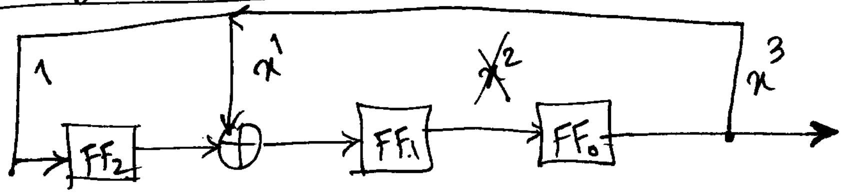
Conclusion: ✗ stream ciphers are not as popular ae block ciphes

✓ like cellphones

crypo secure RNG for stream ciphers

✗ key size = message size

Example-3



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

	FF_2	FF_1	FF_0
	1	1	1
1 →	1	0	1
2 →	1	0	0
3 →	0	1	0
4 →	0	0	1

⋮