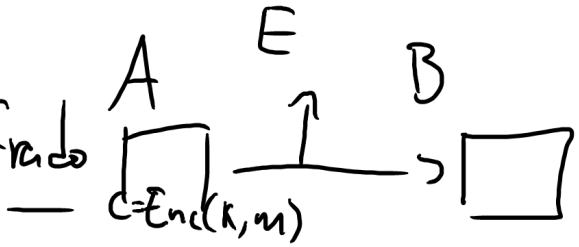
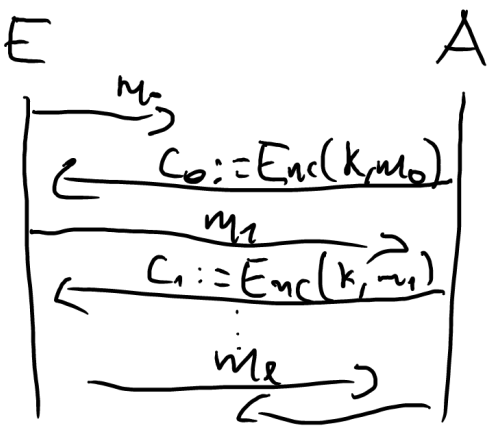
Ataques:

1) Texto cifrado



2) Texto plano E tiene m_0 y $c_0 := \underline{Enc}(k, m_0)$

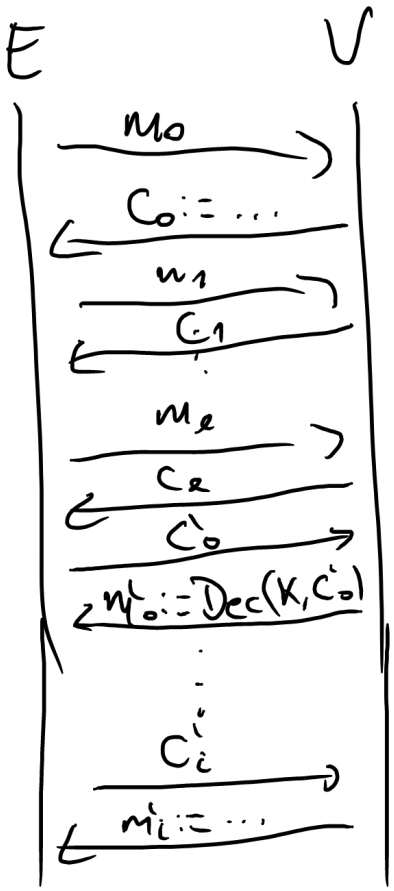
3) Texto plano elegido



E gana si puede producir $m_{\ell+1}$ con su $c_{\ell+1}$ respectivo.

4) Texto cifrado elegido

4) Texto cifrado elegido



E gana igual que en el ataque de texto plano elegido.

Operación Módulo:

Dados $a, n \in \mathbb{Z}$. $\exists! (q, r) \in \mathbb{Z}^2$ tal

Dados $a, n \in \mathbb{Z}$, $\exists! (q, r) \in \mathbb{Z}^2$ tal que:

$a = q \cdot n + r$ y $0 \leq r < |n|$

(q: cociente, r: resto)

Por ejemplo:

$9 \bmod 3 = 0$

$10 \bmod 3 = 1$

$20 = 14 \quad -6 = q \cdot 20 + r$ (-1, 14)

$-6 \bmod -20 = 14 \quad -6 = q \cdot -20 + r$ (1, 14)

$6 \bmod -20 = 6$

$6 = q \cdot -20 + r$ (0, 6)

One-time Pad (OTP)

M = espacio de mensajes

C = espacio de mensajes encriptados

K = espacio de llaves

K = espacio de llaves

(Gen, Enc, Dec)

en OTP

$G := U(K)$

↳ elegir llave uniformemente

$M := \Sigma^l$

$C := \Sigma^l$

$\Sigma := \{0, .., 9, A, .., Z\}$,

Ejemplo con $l = 7$:

$m = 11C3Z53$

$c = AF1CBZ4$

Mapeamos Σ a $\{0, .., |\Sigma|-1\}$

$0, .., 9, A, ..., Z$

$\downarrow 0, .., \downarrow 9, \downarrow 10, ..., \downarrow 35$

$m =$ 1 1 C 3 Z

5 3

5 3

18 18 12 3 2

5 3

K = A F 1 C B Z

4

+ 10 15 1 12 11

35 4

mod 35 28 33 13 15 13

40 7

$(m + k) \bmod 36 =$ 28 33 13 15 13 4

7

$Enc(k, m) :=$ S W D F D 4

7 = C

$Dec(k, c) := (c - k) \bmod 36$

S W D F D 4 7

28 33 13 15 13 4 7

A F 1 C B Z 4

10 15 1 12 11 35 4

	10	15	1	12	11	35	4
c ÷ k	18	18	12	3	2	-31	3
mod 36	18	18	12	3	2	5	3
	1	1	C	3	2	5	3