Introduction to Modern Cryptography

5th lecture:

Message Authentication Codes (MACs) and CCA security

Motivation

- company order
- email, SMS, etc.
- banking transaction
- contracts
- software patches
- ...

integrity and authenticity are often more basic needs than secrecy

Mihir Bellare

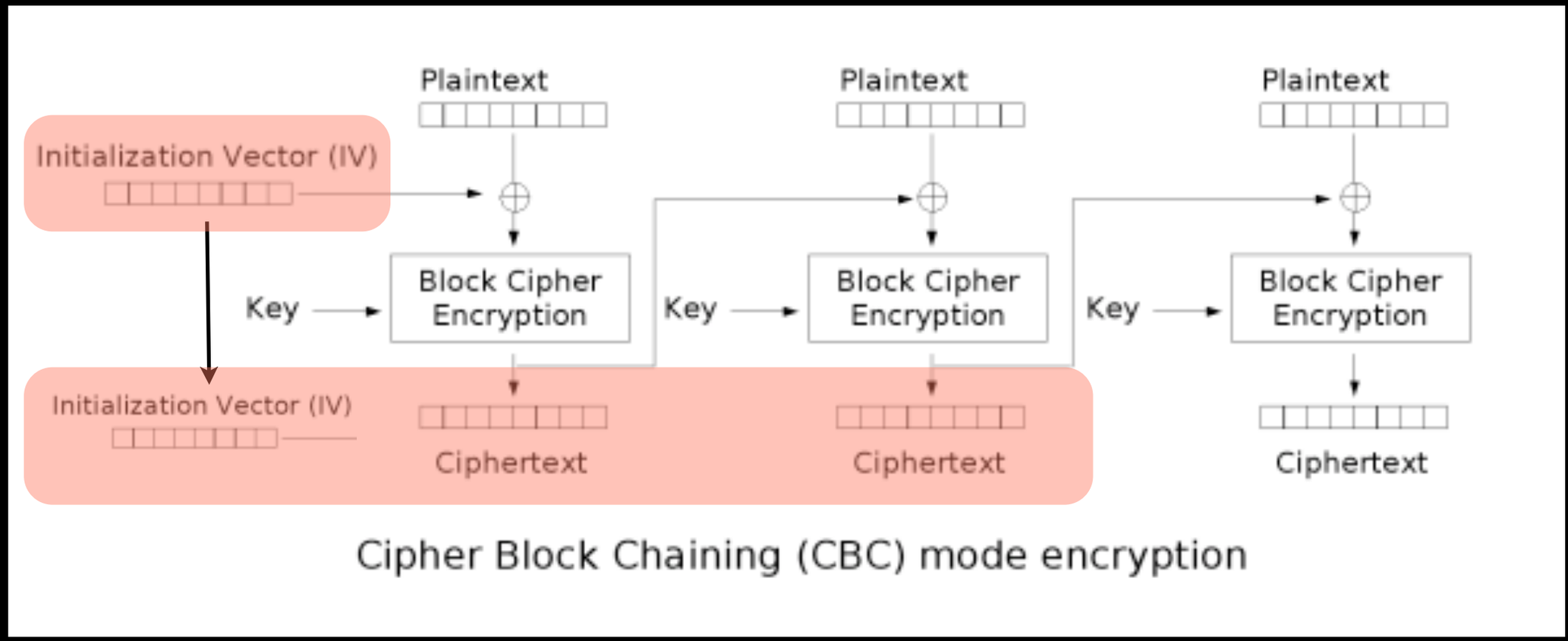
Phillip Rogaway

2000:

- security definition of MACs
- security of CBC MAC

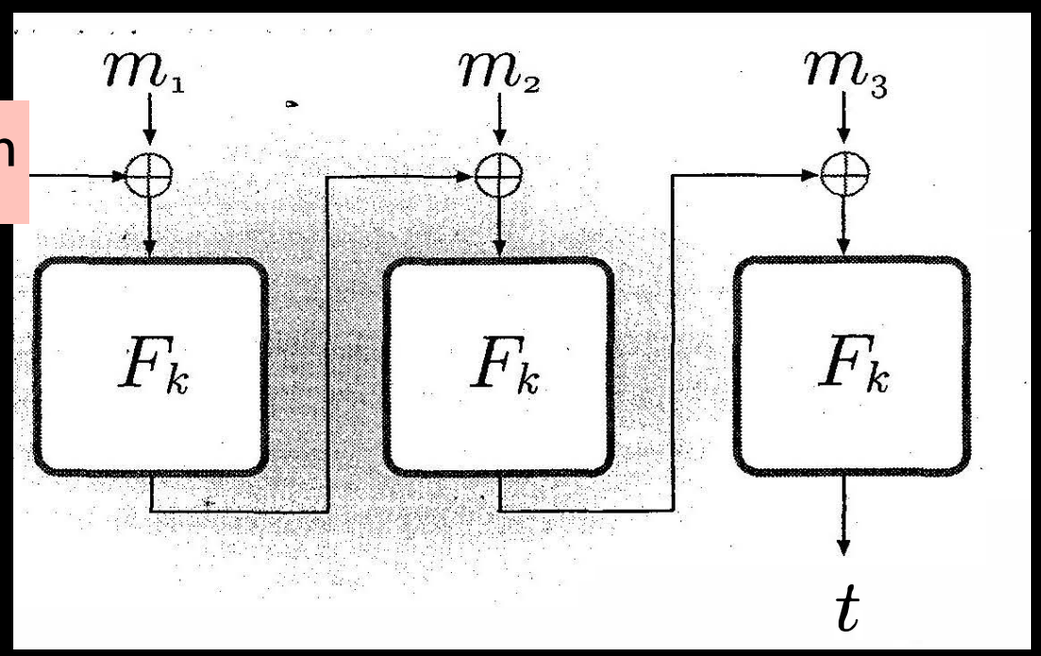
UC Davis, San Diego

CBC encrypt vs CBC-MAC



Cipher Block Chaining (CBC) mode encryption

$t_0 = 0^n$



tricky details!

see exercises

Chosen Ciphertext Attacks (CCA)

$$\mathrm{PrivK}^{\mathrm{cca}}_{\mathcal{A},\Pi}(n)$$

adversary A

challenger

1^n

m_0 , m_1

$\leftarrow A^{Enc_k(\cdot),Dec_k(\cdot)}(1^n)$

$|m_0|=|m_1|$

m_0 , m_1

$k \leftarrow Gen(1^n)$

$b \leftarrow \{0,1\}$

$c \leftarrow Enc_k(m_b)$

c

$b' \leftarrow A^{Enc_k(\cdot),Dec_k(\cdot)}(c)$

b'

adv A cannot ask to decrypt c !

$b=b'$

$b \neq b'$

1

0