

# Introduction to Modern Cryptography



5th lecture:

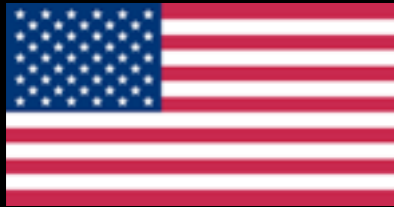
Message Authentication Codes  
(MACs) and CCA security

# 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

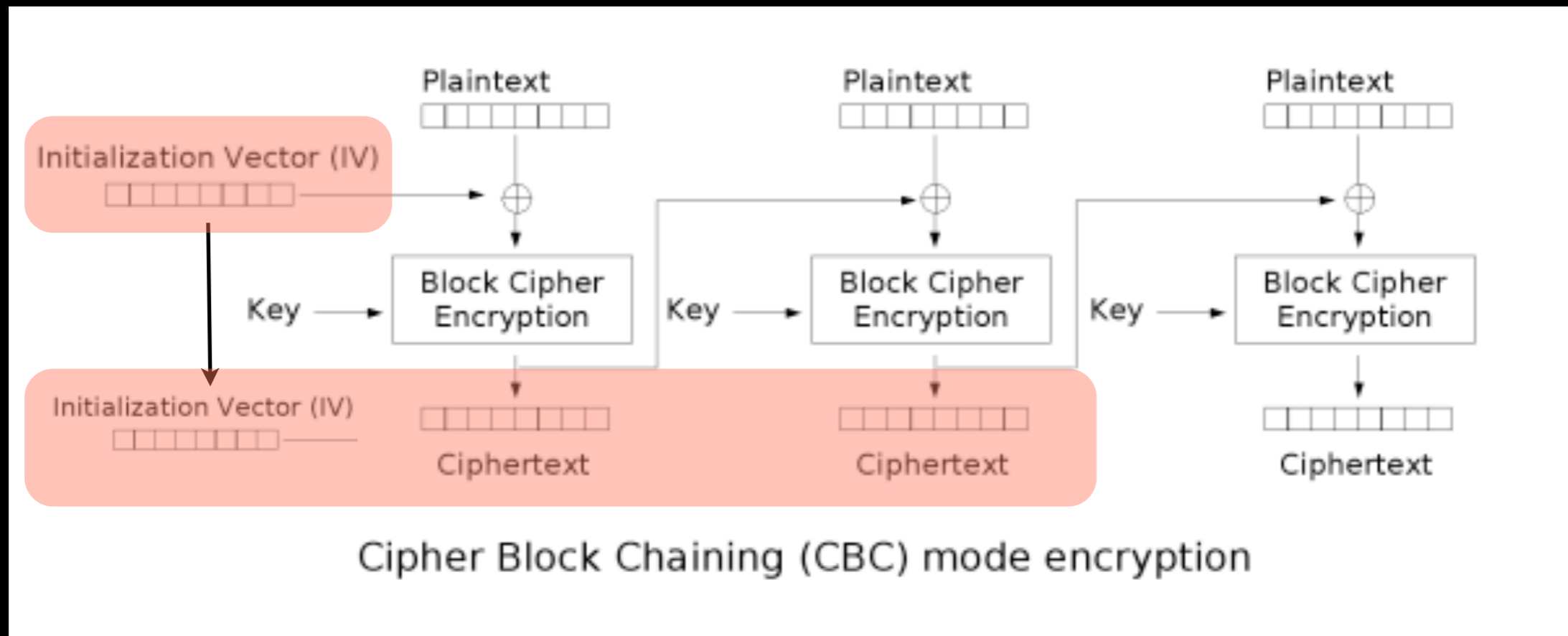


2000:

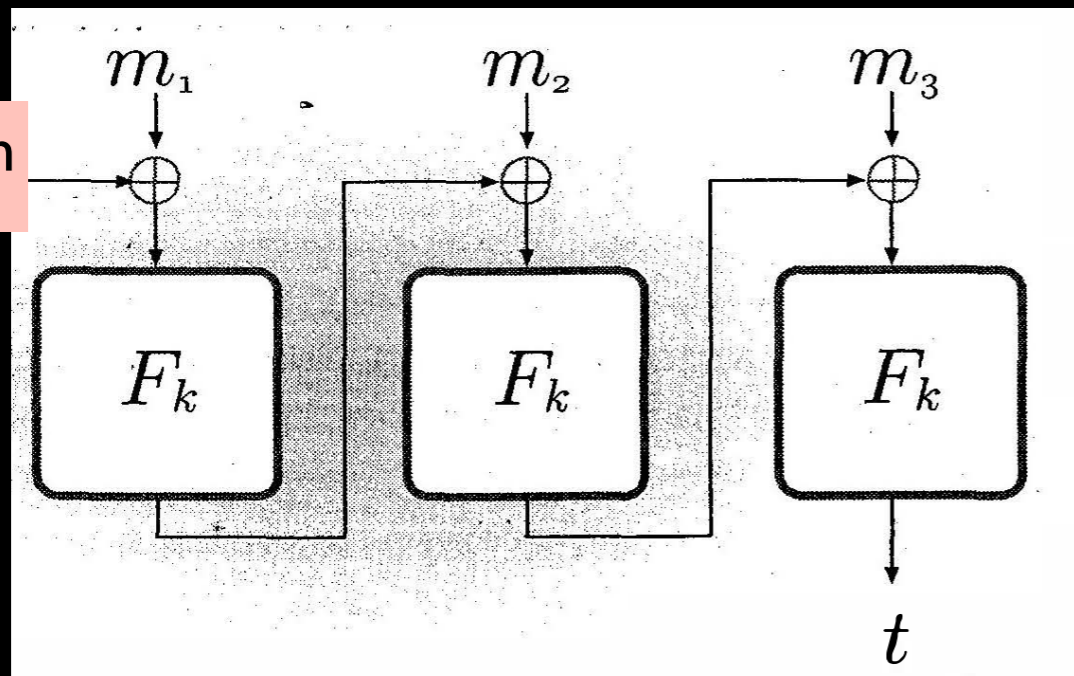
- security definition of MACs
- security of CBC MAC

UC Davis, San Diego

# CBC encrypt vs CBC-MAC



$$t_0 = 0^n$$



tricky details!  
see exercises

# Chosen Ciphertext Attacks (CCA)

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

adversary  $A$

challenger

$m_0, m_1$

$\leftarrow A^{\text{Enc}_k(\cdot), \text{Dec}_k(\cdot)}(I^n)$

$|m_0| = |m_1|$

$b' \leftarrow A^{\text{Enc}_k(\cdot), \text{Dec}_k(\cdot)}(c)$

$I^n$

$m_0, m_1$

$c$

$b'$

$k \leftarrow \text{Gen}(I^n)$

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

$c \leftarrow \text{Enc}_k(m_b)$

$b = b'$

$b \neq b'$

adv  $A$  cannot ask  
to decrypt  $c$  !

↓  
1

↓  
0