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
2000:
• security definition of MACs
• security of CBC MAC

UC Davis, San Diego
CBC encrypt vs CBC-MAC

Cipher Block Chaining (CBC) mode encryption

 Initialization Vector (IV)

Key

Block Cipher Encryption

Ciphertext

Plaintext

Initialization Vector (IV)

Key

Block Cipher Encryption

Ciphertext

Plaintext

Initialization Vector (IV)

Key

Block Cipher Encryption

Ciphertext

Plaintext

$ t_0 = 0^n $

$ m_1 $

$ m_2 $

$ m_3 $

$ F_k $

$ F_k $

$ F_k $

$ t $

tricky details!
see exercises
Chosen Ciphertext Attacks (CCA)

PrivK^{cca}_{A,Π}(n)

adversary A

m_0, m_1 \leftarrow A^{Enc_k(\cdot), Dec_k(\cdot)}(1^n)

|m_0| = |m_1|

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

challenger

k \leftarrow \text{Gen}(1^n)

b \leftarrow \{0, 1\}

c \leftarrow Enc_k(m_b)

b = b'

adv A cannot ask to decrypt c!

b \neq b'

l

0