Introduction to Modern Cryptography

5th lecture:

Message Authentication Codes (MACs) and CCA security last time:

- pseudorandom functions
- chosen-plaintext security

5th lecture (today):

- Message Authentication Codes (MACs)
- CCA security

	secret key	public key
confidentiality	private-key encryption	public-key encryption
authentication	message authentication codes (MAC)	digital signatures

Motivation

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

integrity and authenticity are often more basic needs than secrecy

Mihir Bellare

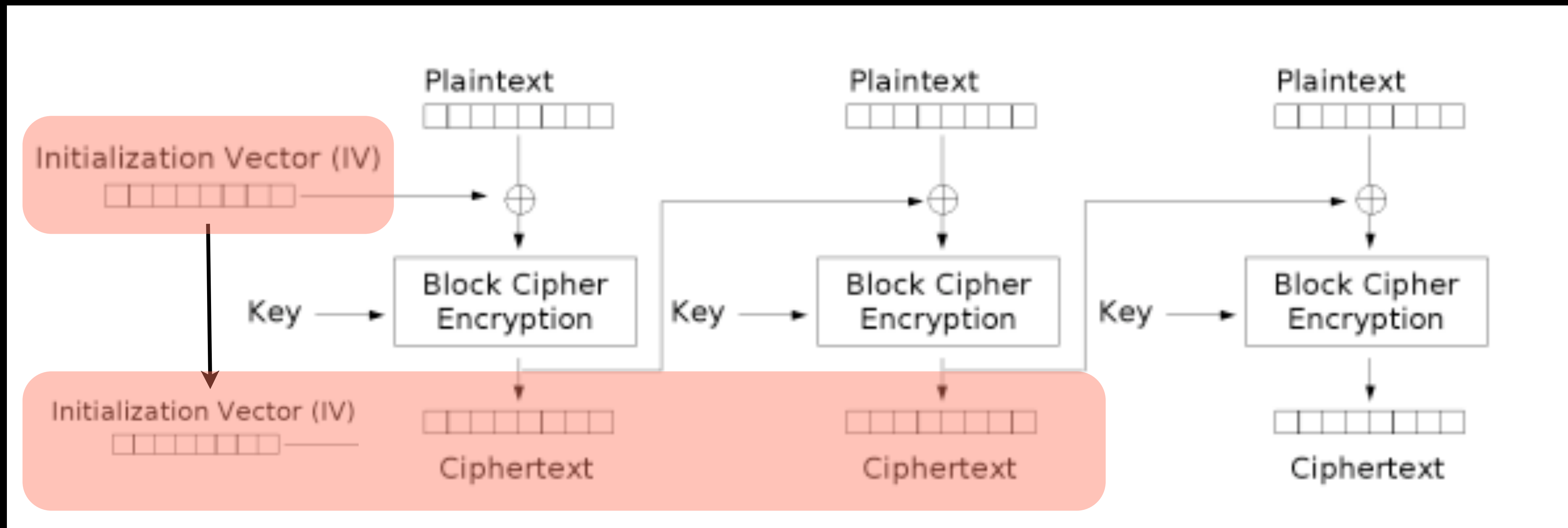
Phillip Rogaway

2000:

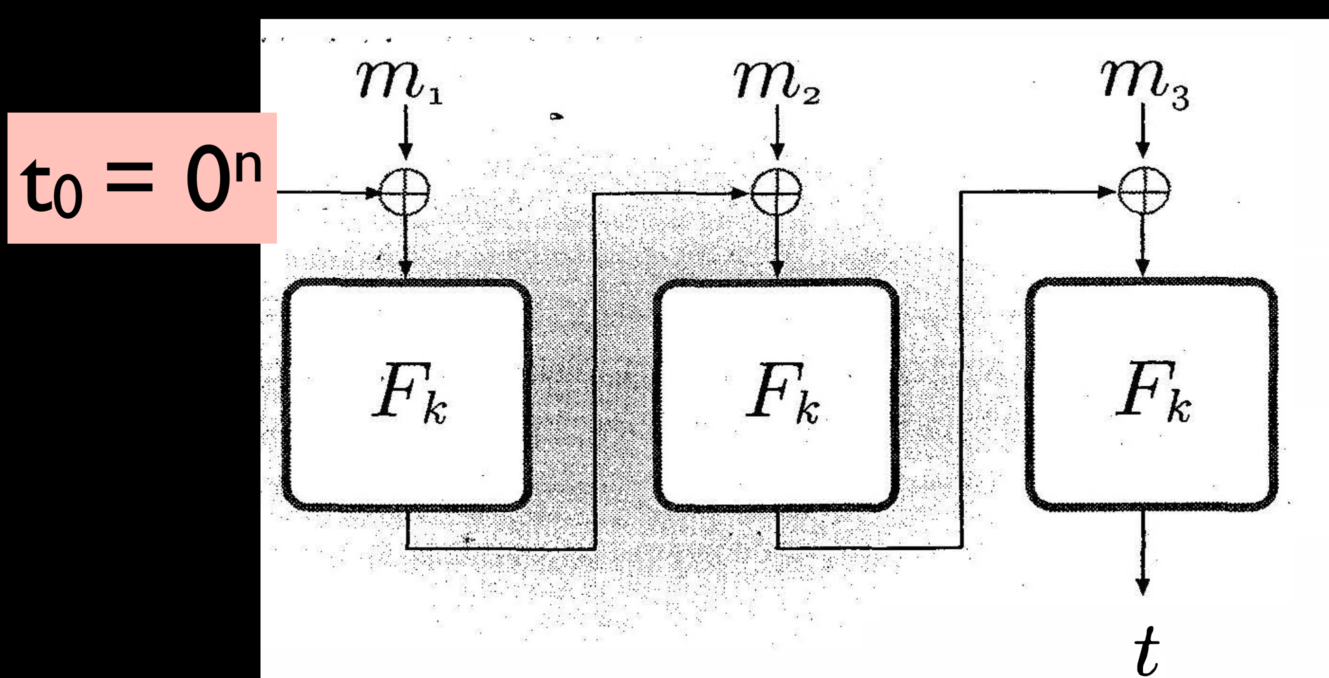
- security definition of MACs
- security of CBC MAC

UC Davis, San Diego

CBC encrypt vs CBC-MAC



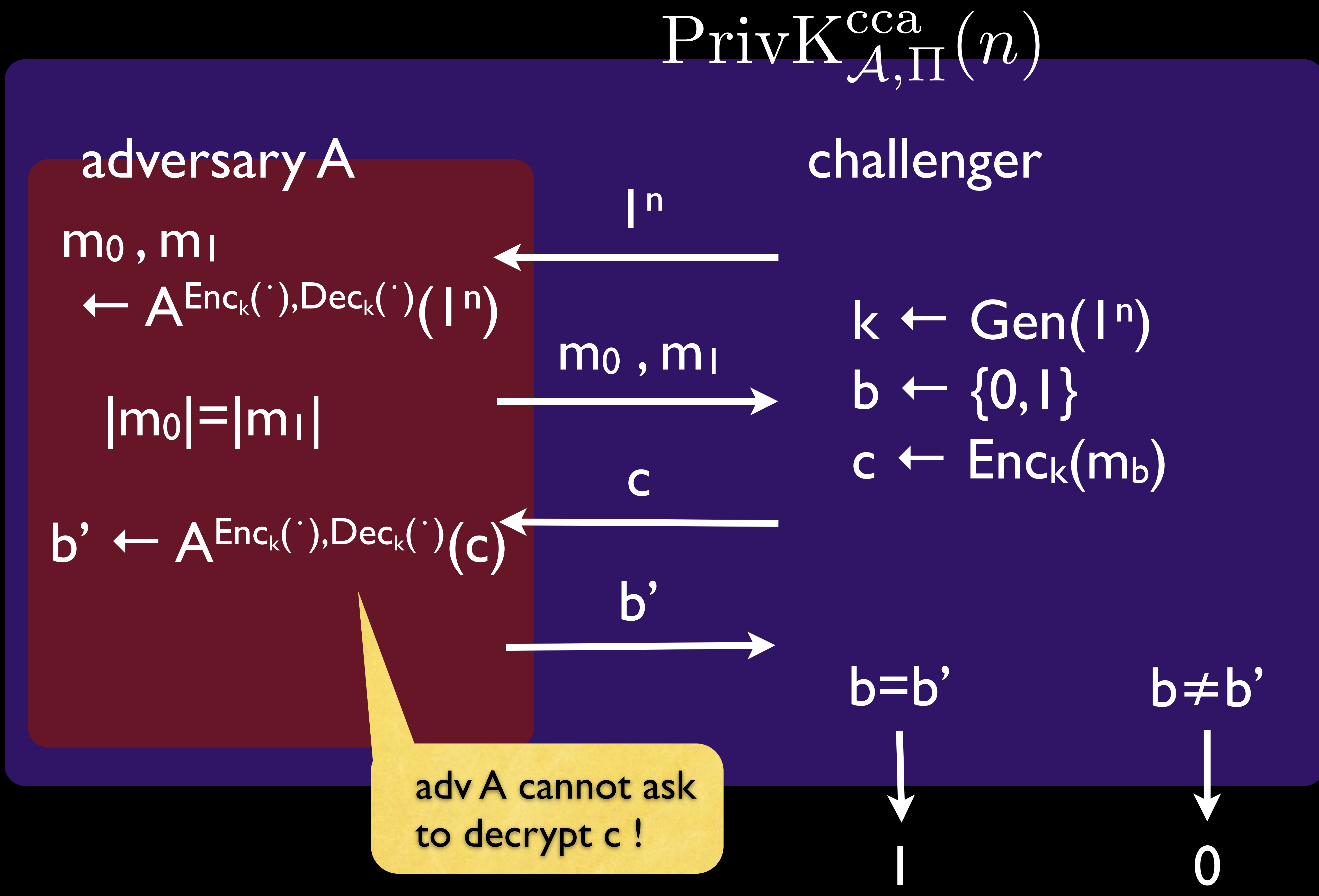
Cipher Block Chaining (CBC) mode encryption



tricky details!

see exercises

Chosen Ciphertext Attacks (CCA)



Trouble with AuthThenEncrypt

$c \leftarrow Enc_{k1}(m \,||\, Mac_{k2}(m))$

$Trans(0) = 00$
$Trans(1) = 01$ or 10

$Trans^{-1}(00) = 0$
$Trans^{-1}(01) = 1$
$Trans^{-1}(10) = 1$
$Trans^{-1}(11) = \perp$

$Enc_k(m) = Enc'_k(Trans(m)) = (r,\ F_k(r) \oplus Trans(m))$

Enc is CPA-secure, but AtE can be CCA-attacked!

$c = Enc'_{k1}(Trans(m||Mac_{k2}(m)))$
$= (r,\ F_k(r) \oplus Trans(m||Mac_{k2}(m)))$

Trouble with AuthThenEncrypt

$c \leftarrow \mathrm{Enc}_{k1}(\ m \ || \ \mathrm{Mac}_{k2}(m)\ )$

$\mathrm{Trans}(0) = 00$

$\mathrm{Trans}(1) = 01$ or 10

$\mathrm{Trans}^{-1}(00) = 0$

$\mathrm{Trans}^{-1}(01) = 1$

$\mathrm{Trans}^{-1}(10) = 1$

$\mathrm{Trans}^{-1}(11) = \perp$

CTR-mode with PRF F_k

$\mathrm{Enc}_k(m) = \mathrm{Enc}'_k(\mathrm{Trans}(m)) = (\ r,\ F_k(r) \oplus \mathrm{Trans}(m)\ )$

Enc is CPA-secure, but AtE can be CCA-attacked!

$c = \mathrm{Enc}'_{k1}(\ \mathrm{Trans}(m || \mathrm{Mac}_{k2}(m))\ )$

$\quad = (\ r,\ F_k(r) \oplus \mathrm{Trans}(m || \mathrm{Mac}_{k2}(m))\ )$

Trouble with AuthThenEncrypt

$c \leftarrow Enc_{k1}(\ m\ ||\ Mac_{k2}(m)\ )$

$Trans(0) = 00$

$Trans(1) = 01$ or 10

$Trans^{-1}(00) = 0$

$Trans^{-1}(01) = 1$

$Trans^{-1}(10) = 1$

$Trans^{-1}(11) = \perp$

CTR-mode with PRF F_k

$Enc_k(m) = Enc'_k(Trans(m)) = (\ r,\ F_k(r) \oplus Trans(m)\ )$

Enc is CPA-secure, but AtE can be CCA-attacked!

$c = Enc'_{k1}(\ Trans(m||Mac_{k2}(m))\ )$

$= (\ r,\ F_k(r) \oplus Trans(m||Mac_{k2}(m))\ )$

flipping the first two bits of this block and trying Dec( ) reveals the first bit of m

Bruce Schneier

- wrote several books and articles about computer security
- influential blog and newsletter
- designed crypto algorithms
- board member of Electronic Frontier Foundation (EFF)

- visit his official site, and the funny Bruce Schneier Facts