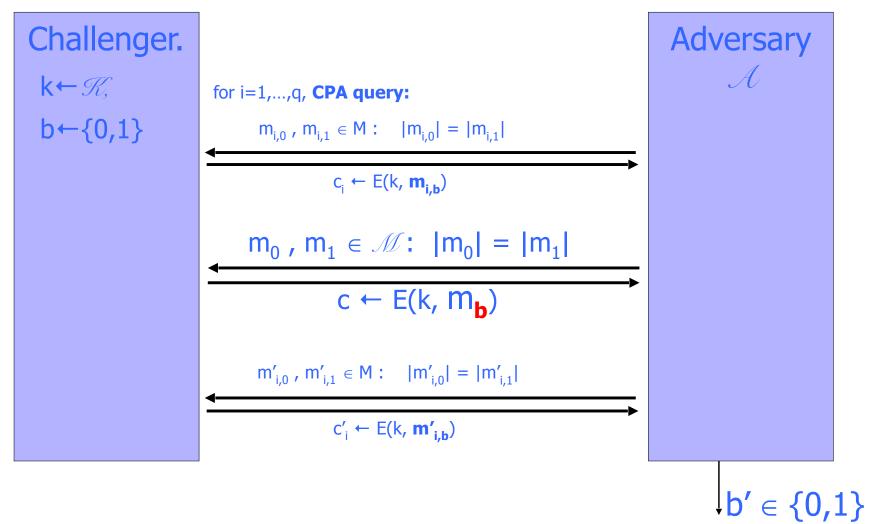
Message Integrity

Yan Huang

CPA Recap

- 1. $k \leftarrow \text{KeyGen}(1^n)$. $b \leftarrow \{0,1\}$. Give $\text{Enc}(k, \cdot)$ to \mathcal{A} .
- 2. \mathcal{A} chooses as many plaintexts as he wants, and receives the corresponding ciphertexts via Enc(k, \cdot).
- 3. \mathcal{A} picks two plaintexts M_0 and M_1 (Picking plaintexts for which A previously learned ciphertexts is allowed!)
- 4. \mathcal{A} receives the ciphertext of M_b , and continues to have accesses to Enc(k, \cdot).
- 5. \mathcal{A} outputs b'.
- \mathcal{A} wins if b'=b.

CPA Recap



For all efficient adversary \mathcal{A} , | Pr[b=b'] - 1/2 | is "negligible".

Motivating Example



Bank of America Accounts Bill Payre Transfors Investments Customer Service Pay Tu/Pay from . Delete Pay To Account: Confirm

Quick Help Pay To Account Information You are about to delete this Pay To assess Bank of America Credit Card Water Pary To. Fay In Bank of America -1467 Payment address on Ne with Dank of America. account details > What can I do? What do I need to know? Payment Schedule Summary > what else can I do? If you have questions, provide our list of frequently arked.

You set up recurring parametes for this Pay To account, which will be canceled when you delete this Pay To account.

Online Banking smott

terra-Bille Inight Incations New Hall : Help

Amount: \$100

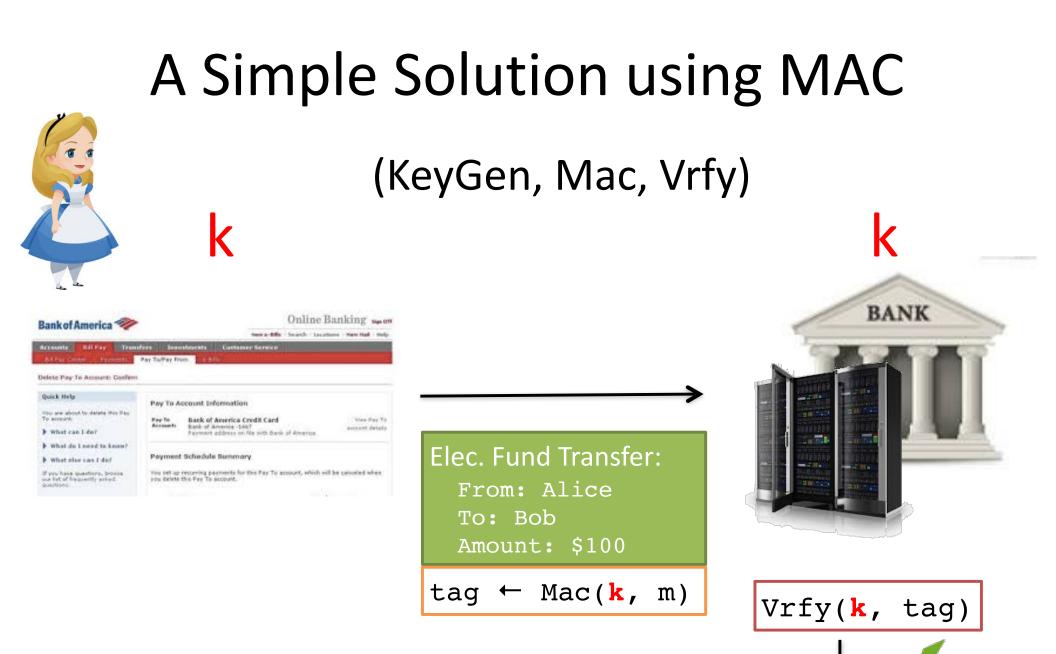
Does Encryption Solve the Problem?



Enc(

Elec. Fund Transfer: From: Alice To: Bob Amount: \$100





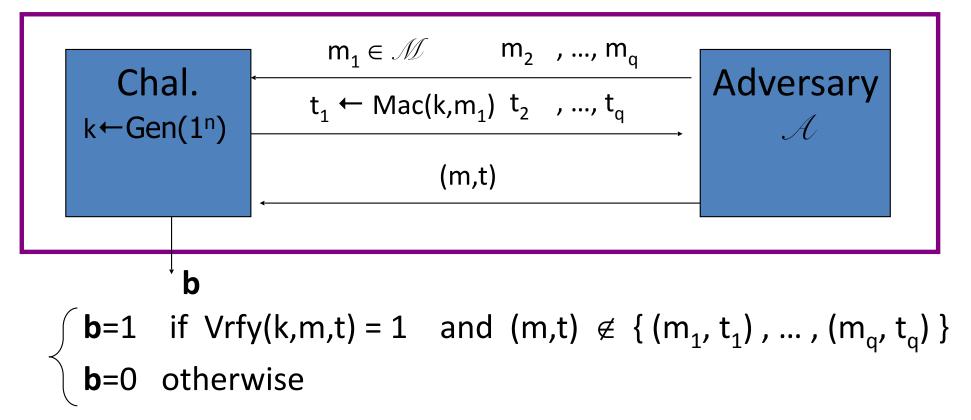
Message Integrity Game

- 1. k \leftarrow Gen(1ⁿ).
- A is given polynomial time and an oracle access to query Mac(k, •). Let t_i=Mac(k, m_i) and Q={(m₁, t₁), ..., (m_q, t_q)}.
 A outputs (m, t).

 \mathcal{A} wins the game if Vrfy(m, t)=1 and $(m,t) \notin Q$.

Message Integrity

(Gen, Mac, Vrfy) --- a message authentication code scheme.



Def: (Gen, Mac, Vrfy) is a <u>Secure Message Authentication</u> <u>Code</u> if for all "efficient" \mathcal{A} :

 $Adv_{Mac}[\mathcal{A}] = Pr[Chal. outputs 1]$ is "negligible."

One block message

Let F be a secure block cipher (i.e., AES).

Mac(k,m) = F(k,m)Vrfy(k,m||t) = 1 iff F(k,m)=t

MAC arbitrary number of blocks

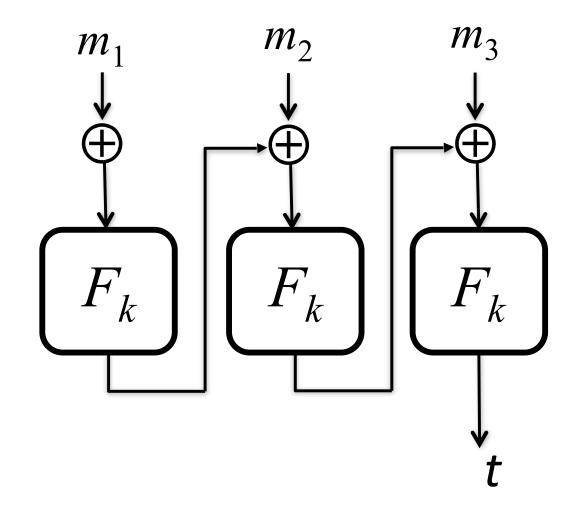
Does this work?

Let F be a secure block cipher (i.e., AES).

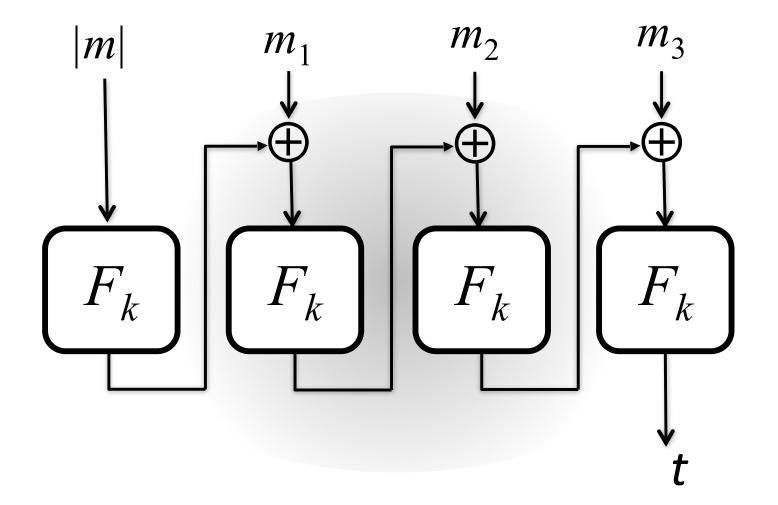
$$m_1$$
 $F_k(m_1)$ m_2 $F_k(m_2)$ m_3 $F_k(m_3)$

 $Mac(k,m) = F_k(m_1), F_k(m_2), F_k(m_3)$

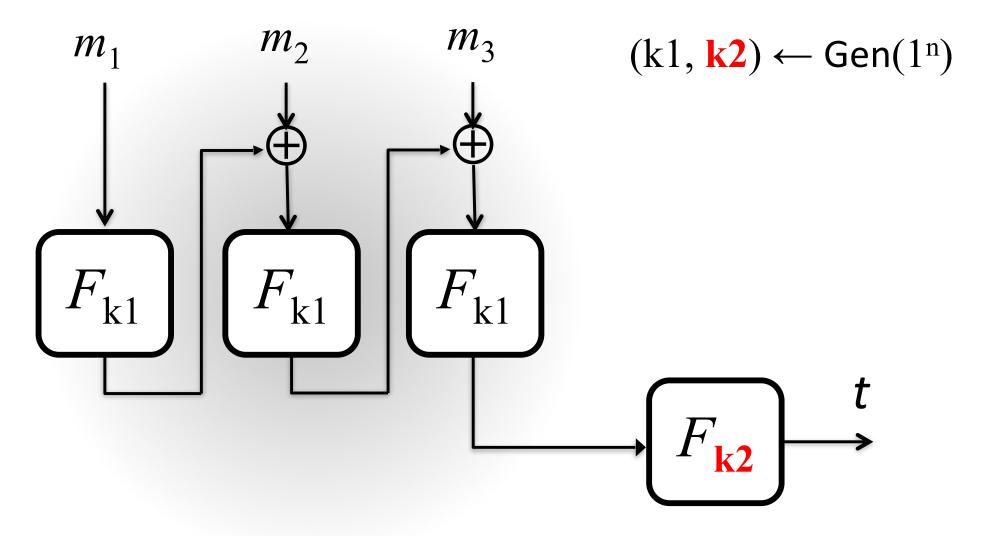
MAC arbitrary number of blocks Is CBC a good MAC?



MAC arbitrary number of blocks Scheme I



MAC arbitrary number of blocks Scheme II



No need to know the length of the message in advance.

Warning!

Even harmless-looking modifications to cryptographic constructions can render them insecure!