Today in Cryptography (5830)

Review of modes of operation & active attacks
Message authentication
CBC-MAC
Attacks against bad CBC-MAC implementations
Variable-length secure CBC-MAC

Review

- **Goal**: secure (length-extending) encryption
- What we have so far:
  - Block cipher modes of operation (CBC, CTR)
  - Insecurity against active attacks
    - Bit flip “mauling” attacks against CTR
    - Padding oracle attacks against CBC

- We need another tool:

  authenticity mechanisms

Malleability example: Encrypted cookies

http://startup.com

GET /index.html HTTP/1.1

HTTP/1.1 200 OK
Content-type: text/html
Set-cookie: sessionToken=ab35h013490...

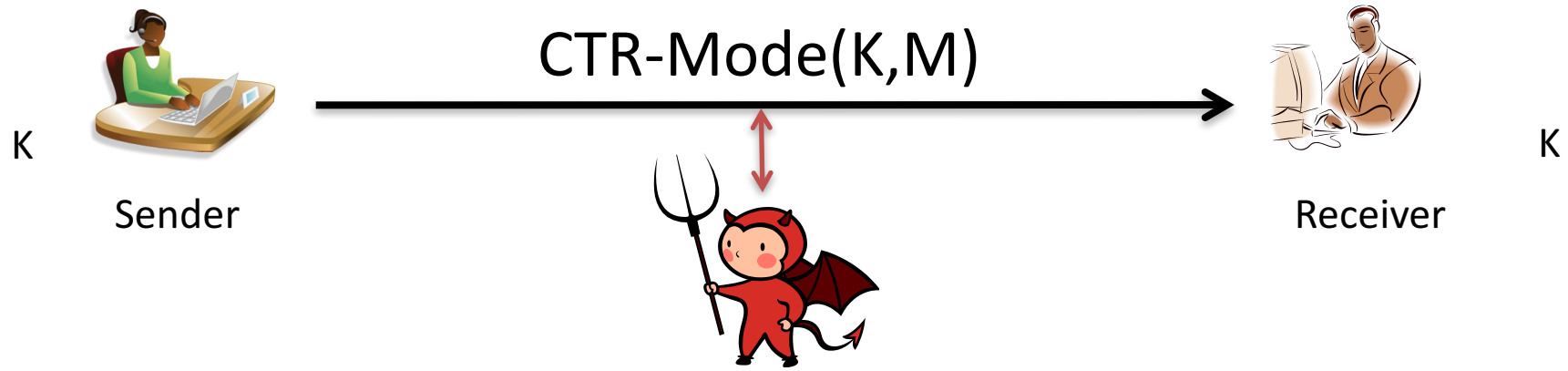
Has secret key K

GET /info.html HTTP/1.1
Cookie: sessionToken=ab35h013490…

abc35h013490… = CTR-Mode(K, “admin=0”)

Malicious client can simply flip a few bits to change admin=1

More generally:

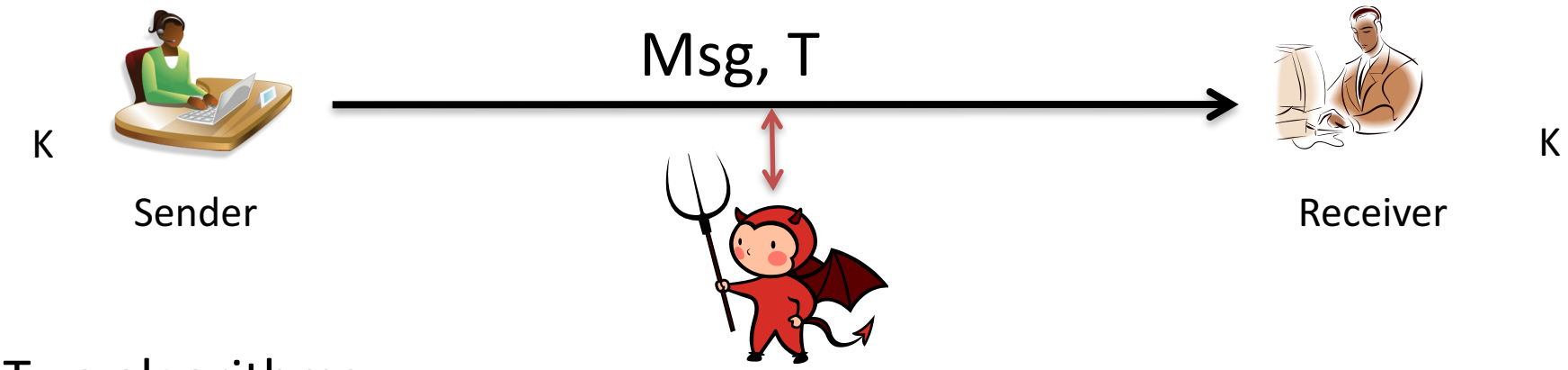


Attacker has read/write access to communications channel

<u>The strategy:</u>

Arrange so that that all bits received can be validated as having come from sender (the person with key K)

The tool: Message authentication



Two algorithms:

(1) Tag(K,Msg) outputs a tag T

(2) Verify(K,Msg,T) outputs 0/1 (invalid / valid)

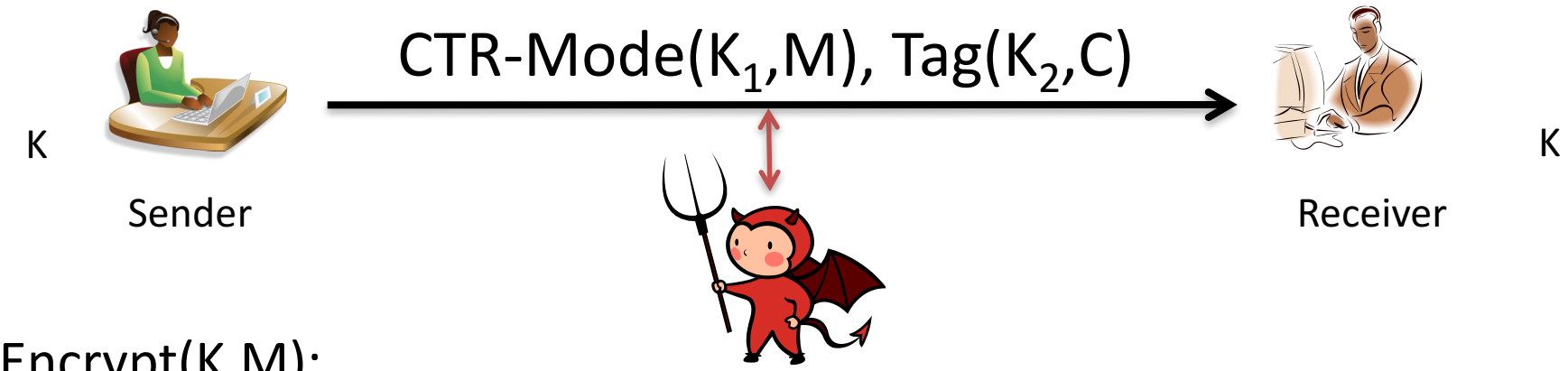
Correctness: Verify(K,Msg,Tag(K,Msg)) = 1 always

Security: No computationally efficient attacker can forge tags for a new message even when attacker gets

$(Msg_1 , T_1) , (Msg_2 , T_2), \ldots , (Msg_q , T_q)$

for messages of his choosing and reasonably large q.

Composing encryption and authentication



Encrypt(K,M):

Use secret keys K_1 and K_2 . These can be derived from K if needed

$K_1 = AES(K,0^n)$ $K_2 = AES(K,1^n)$

C = CTR-Mode(K_1, M)

T = Tag(K_2,C)

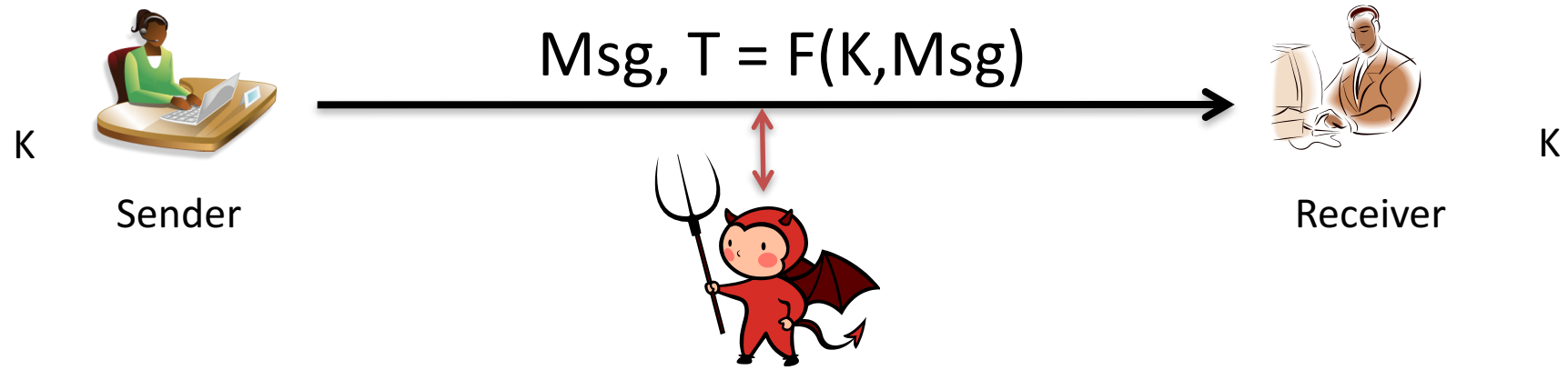
Output C||T

Decrypt(K,C||T)

If Tag(K_2,C,T) ≠ 1 then Return error

Return CTR-Mode(K_1,C)

Message authentication using pseudorandom functions (PRFs)

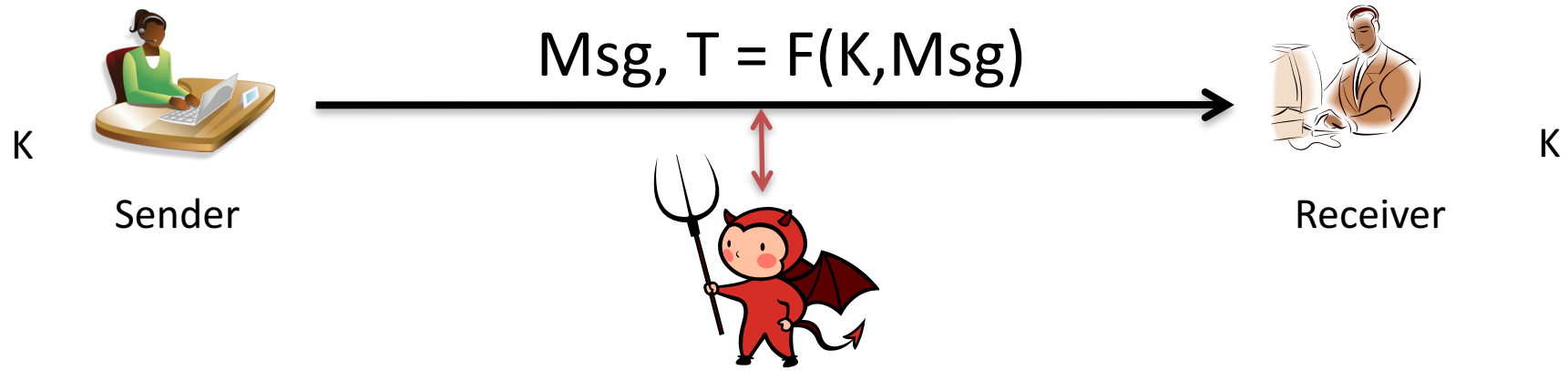


Tag(K,M) = F(K,Msg)

If F behaves like random function (to those w/o K, this will be secure.

What was example of a good PRF?

Message authentication using pseudorandom functions (PRFs)



Tag(K,M) = F(K,Msg)

If F behaves like random function (to those w/o K, this will be secure.

Deterministic message authentication scheme is often called *message authentication code (MAC)* and tag called MAC

What was example of a good PRF?

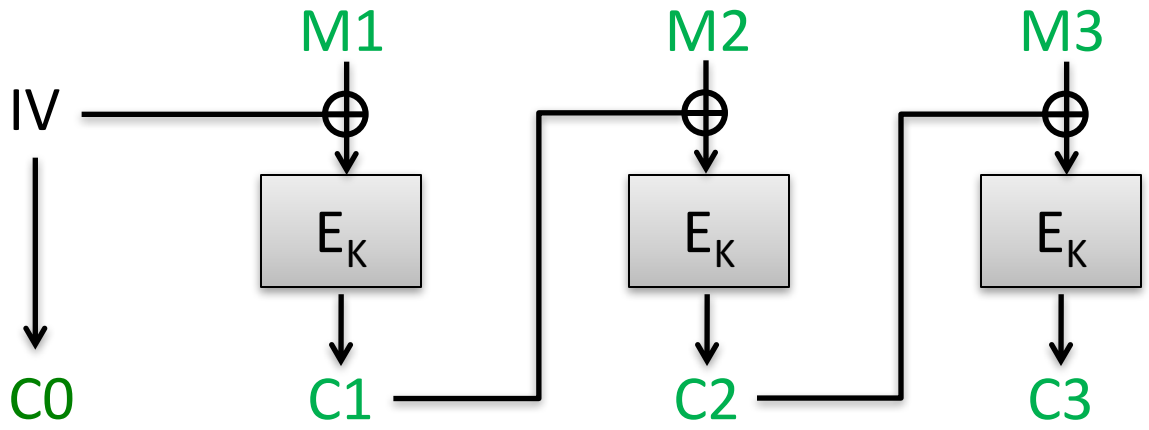
Recall CBC mode

Ciphertext block chaining (CBC)

Pad message M to M1,M2,M3,... where each block Mi is n bits

Choose random n-bit string IV

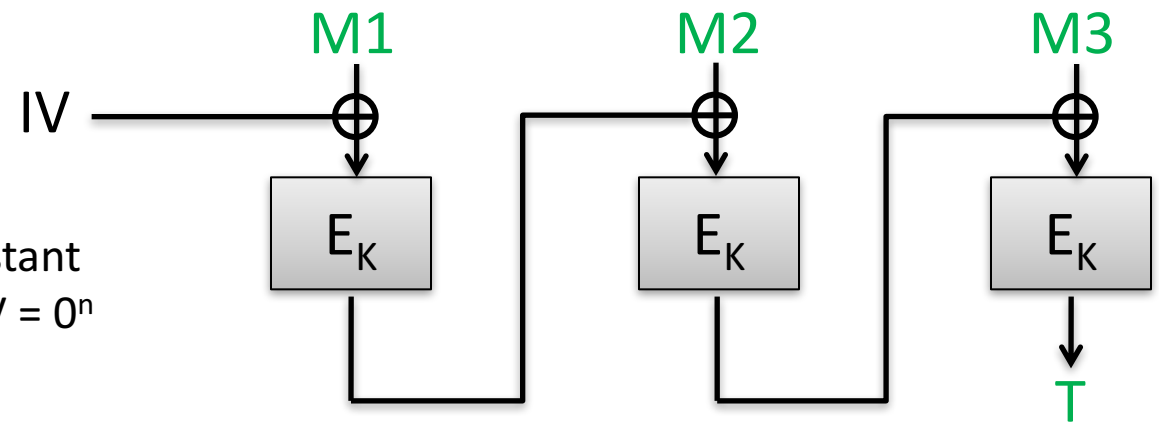
Then:



Can we convert this into variable-message-length PRF?

CBC-MAC

Message authentication code (MAC)



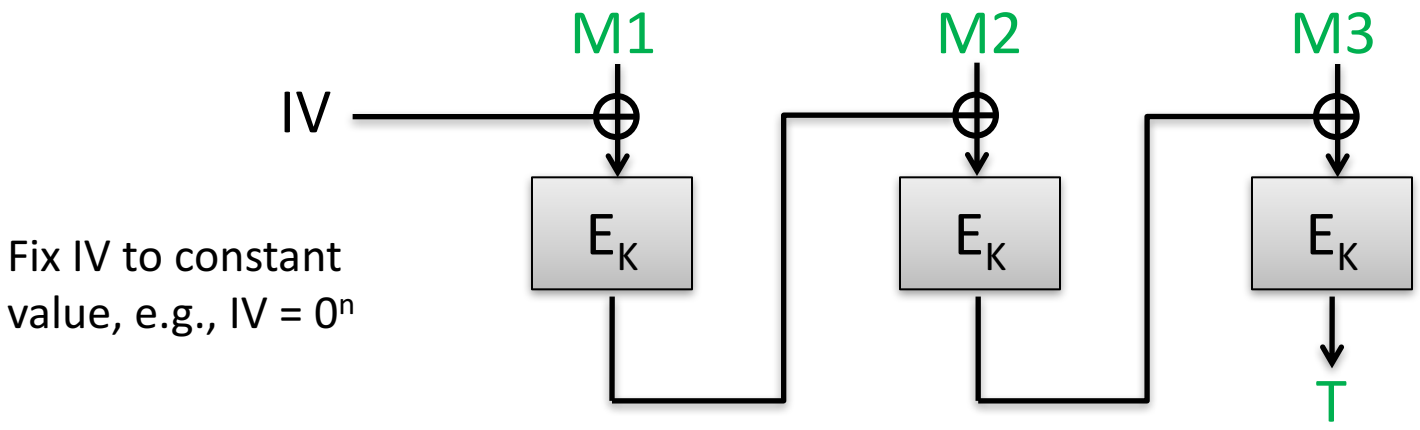
Fix IV to constant value, e.g., IV = 0^n

Turns out this is (provably) a good PRF

if only K used only on same-length messages

CBC-MAC

Message authentication code (MAC)

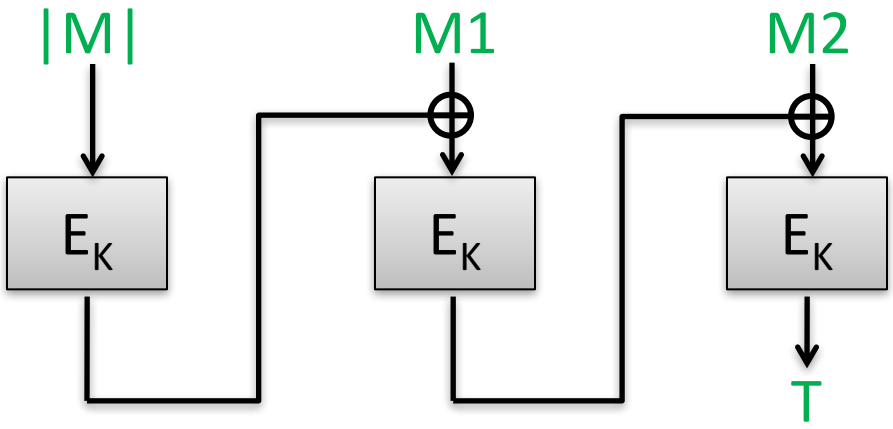


Turns out this is (provably) a good PRF

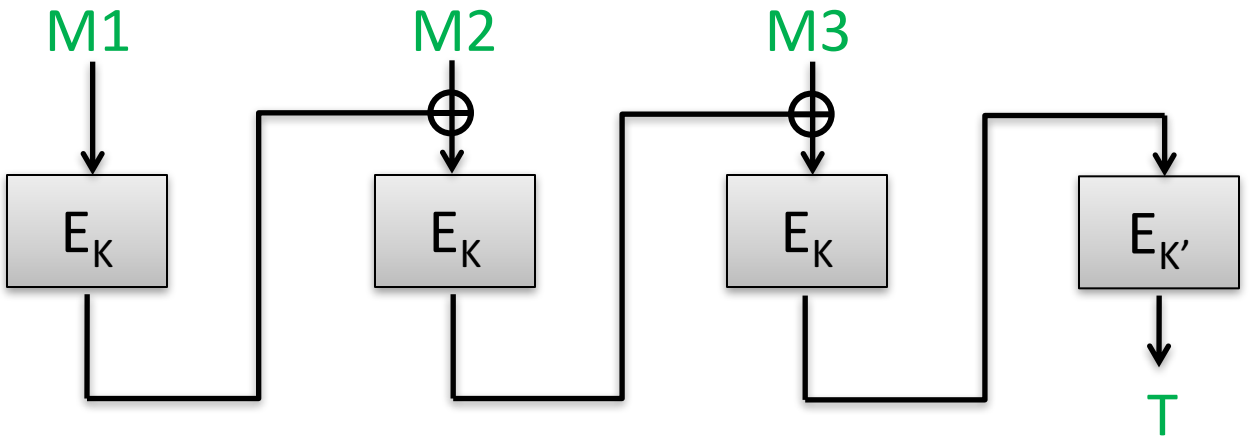
if K used only on same-length messages

Variable-message-length CBC-MAC

- Prepend message length



- Encrypted CBC-MAC



Discussion exercise

- We used hazmat interface for CBC mode in HW1 to implement Feistel round function.

- Does this realize a secure implementation of CBC-MAC?