THE VERGE

ars technica

FCC fines Verizon $1.35 million over 'supercookie' tracking

By Jacob Kastrenakes on March 7, 2016 12:43 pm

Verizon is giving a new mission to its controversial hidden identifier that tracks users of mobile devices. Verizon said in a little-noticed announcement that it will soon begin sharing the profiles with AOL's ad network, which in turn monitors users across a large swath of the Internet.

That means AOL's ad network will be able to match millions of Internet users to their real-world details gathered by Verizon, including "your gender, age range and interests." AOL's network is on 40 percent of websites, including on ProPublica.

AOL will also be able to use data from Verizon's identifier to track the apps that mobile users open, what sites they visit, and for how long. Verizon purchased AOL earlier this year.

Verizon, which has 135 million wireless customers, says it will share the identifier with "a very limited number of other partners and they will only be able to use it for Verizon and AOL purposes," said Karen Zacharia, chief privacy officer at Verizon.

In order for the tracking to work, Verizon needs to repeatedly insert the identifier into users' Internet traffic. The identifier can't be inserted when the traffic is encrypted, such as when a user logs into their bank account.

public key *cryptography*

cs642

adam everspaugh
ace@cs.wisc.edu

computer security

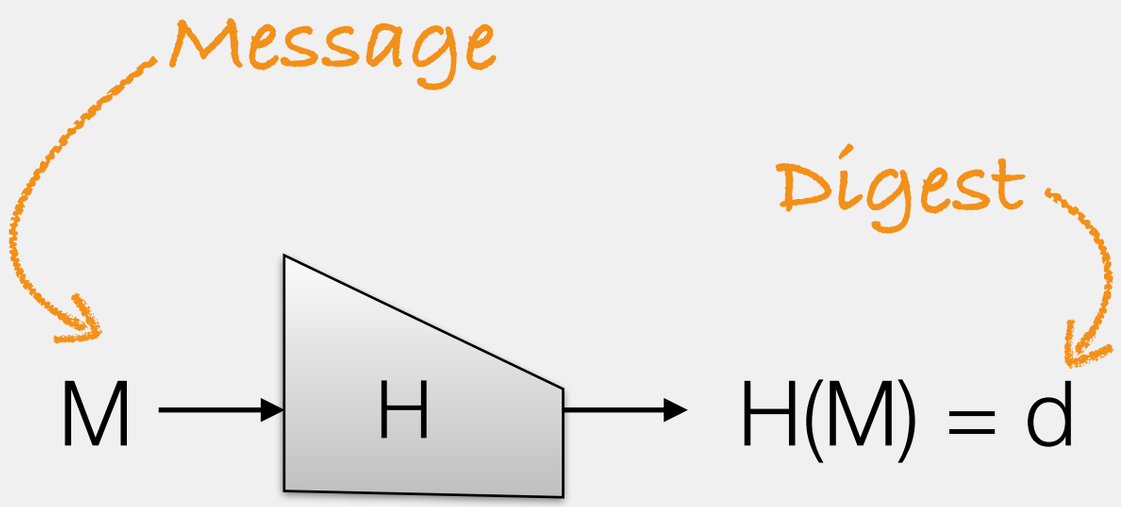
announcements

* HW2 posted, due March 28
* Should be fun!

today

* Hash functions, HMAC
* Authenticated encryption
* Public key cryptography
  * Pubkey encryption, hybrid encryption
  * Digital signatures, certificates

hash functions



$H: \{0,1\}^* \rightarrow \{0,1\}^m$

Broken:

- MD5 m=128
- SHA-1 m=160

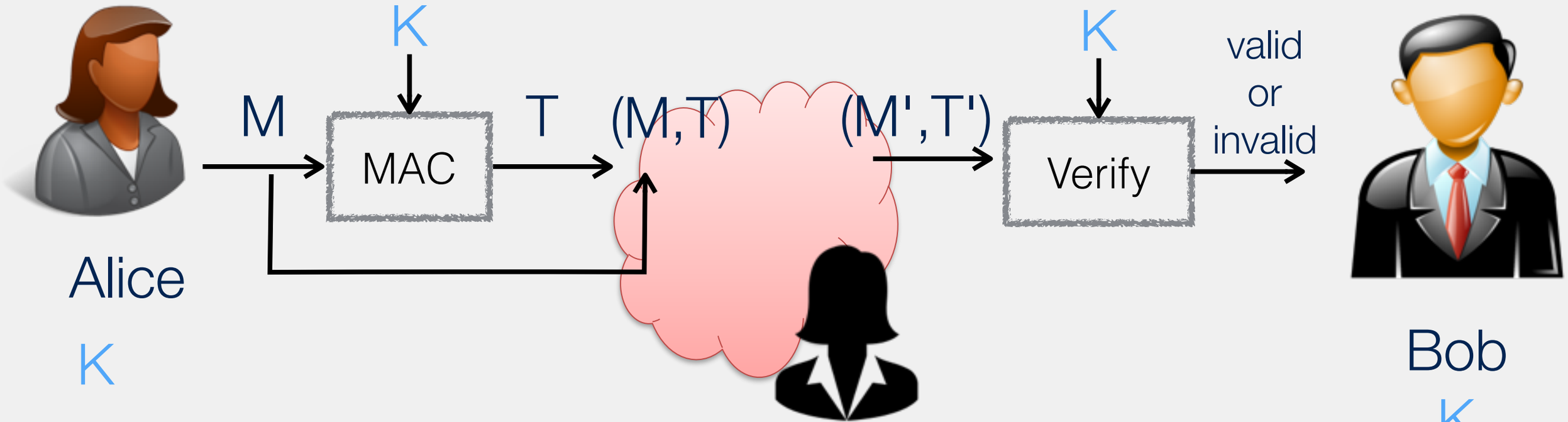
Current:

- SHA-256 m=256
- SHA-512 m=512
- SHA3-256/512

Security goals

* **Collision resistance**
  / Hard to find any two messages: m≠m', H(m)=H(m')
* **Second pre-image resistance**
  / Given m, hard to find m'≠m where H(m)=H(m')
* **One-way**
  / Given random d, hard to find m with H(m)=d

hash function



Message Authentication Code (MAC)
message integrity & authenticity / symmetric

* Hashed Message Authentication Code (HMAC)

* Standard method to construct a secure MAC from a hash function H and a key

$$\text{HMAC}(K,M) = H(\, K \oplus \text{opad} \,\|\, H(\, K \oplus \text{ipad} \,\|\, M)\,)$$

Fixed constants
(not tablets made by Apple)

hmac

authenticated encryption

k_1 - encryption key
k_2 - MAC key

$C=E_{k1}(M)$, $T=MAC_{k2}(C)$

C,T

encrypt-then-mac

secure for all secure primitives

think-*pair*-share

encrypt-and-mac

may be insecure

$C=E_{k1}(M)$, $T=MAC_{k2}(M)$

C,T

mac-then-encrypt

may be insecure

$T=MAC_{k2}(M)$, $C=E_{k1}(M,T)$

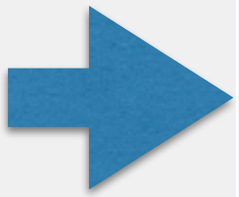
C

Even better: use a dedicated AE mode

authenticated encryption

Dedicated authenticated encryption schemes

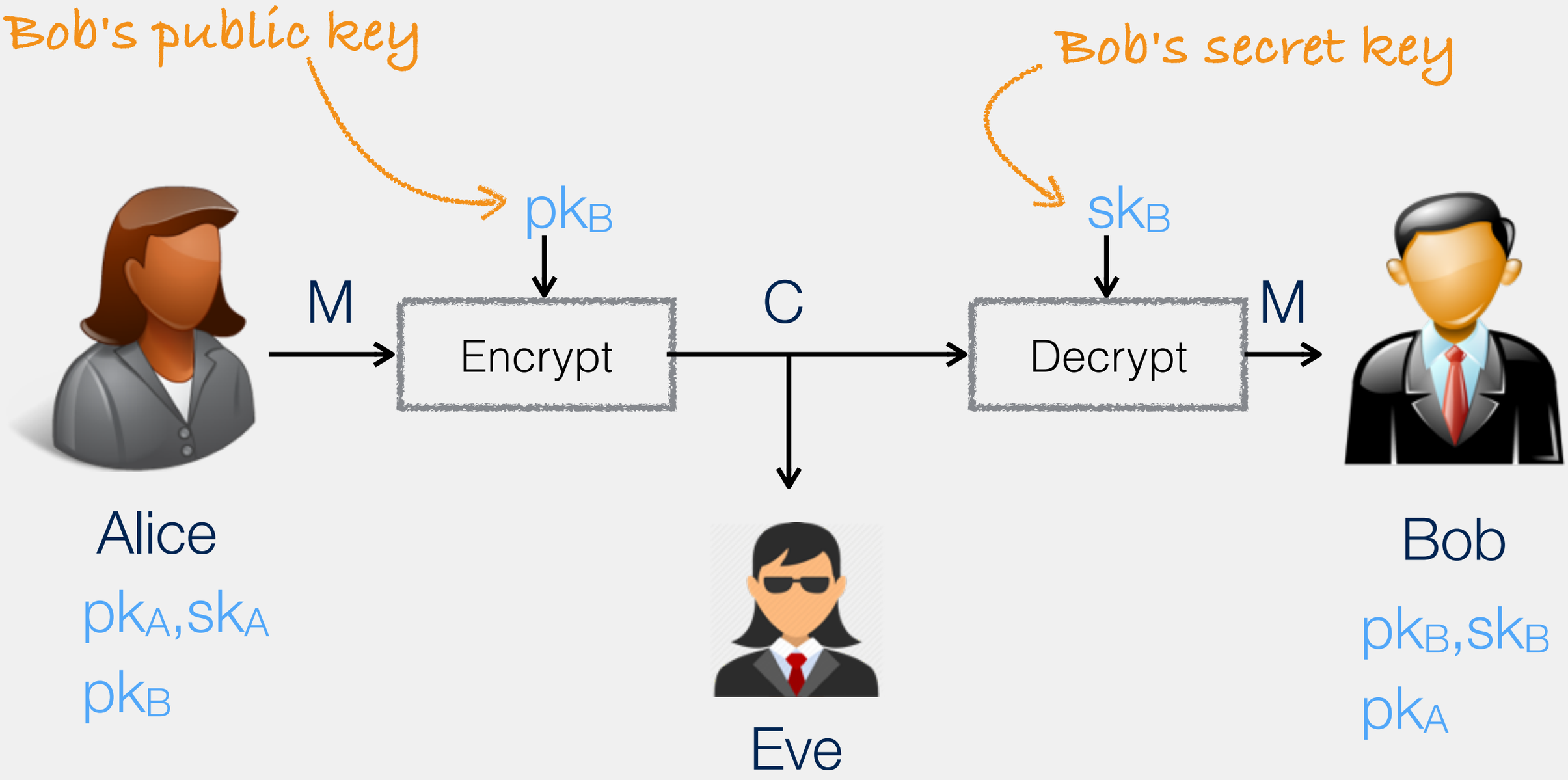
Attack	Inventors	Notes
OCB (Offset Codebook)	Rogaway	One-pass
GCM (Galios Counter Mode)	McGrew, Viega	CTR mode plus specialized MAC
CWC	Kohno, Viega, Whiting	CTR mode plus Carter-Wegman MAC
CCM	Housley, Ferguson, Whiting	CTR mode plus CBC-MAC
EAX	Wagner, Bellare, Rogaway	CTR mode plus OMAC



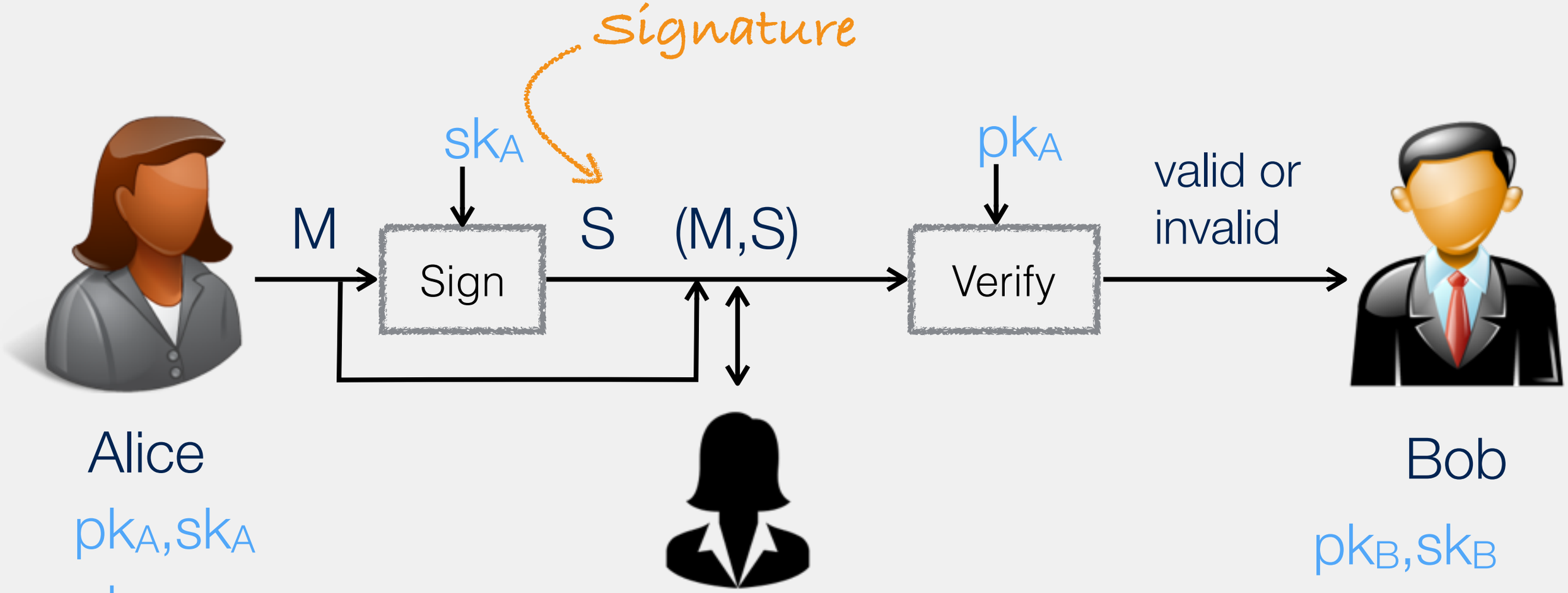
AES-GCM - most common,
built-in instructions in Intel chips (very fast)

ae modes

public key cryptography



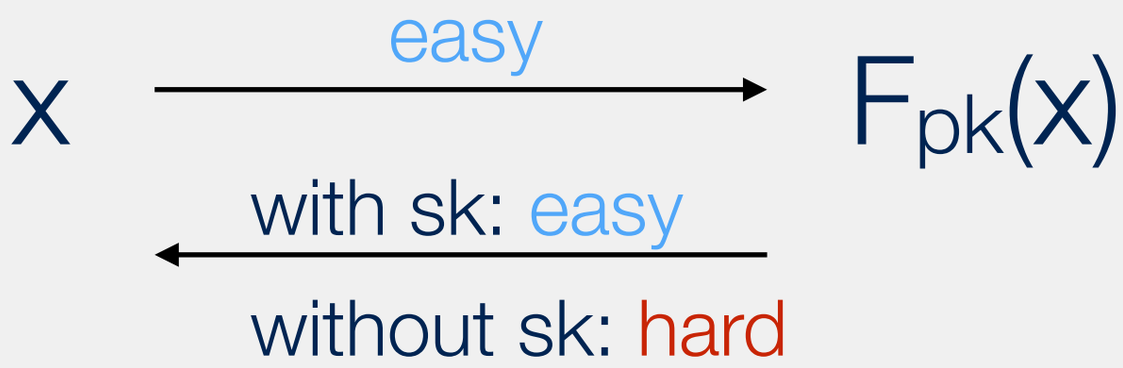
asymmetric encryption



message integrity & authenticity / asymmetric

digital signatures

Kg → (pk,sk)



Trapdoor function

F_{pk}: X→Y

F^{-1}_{sk}: Y→X

Trapdoor permutation

F_{pk}: X→X

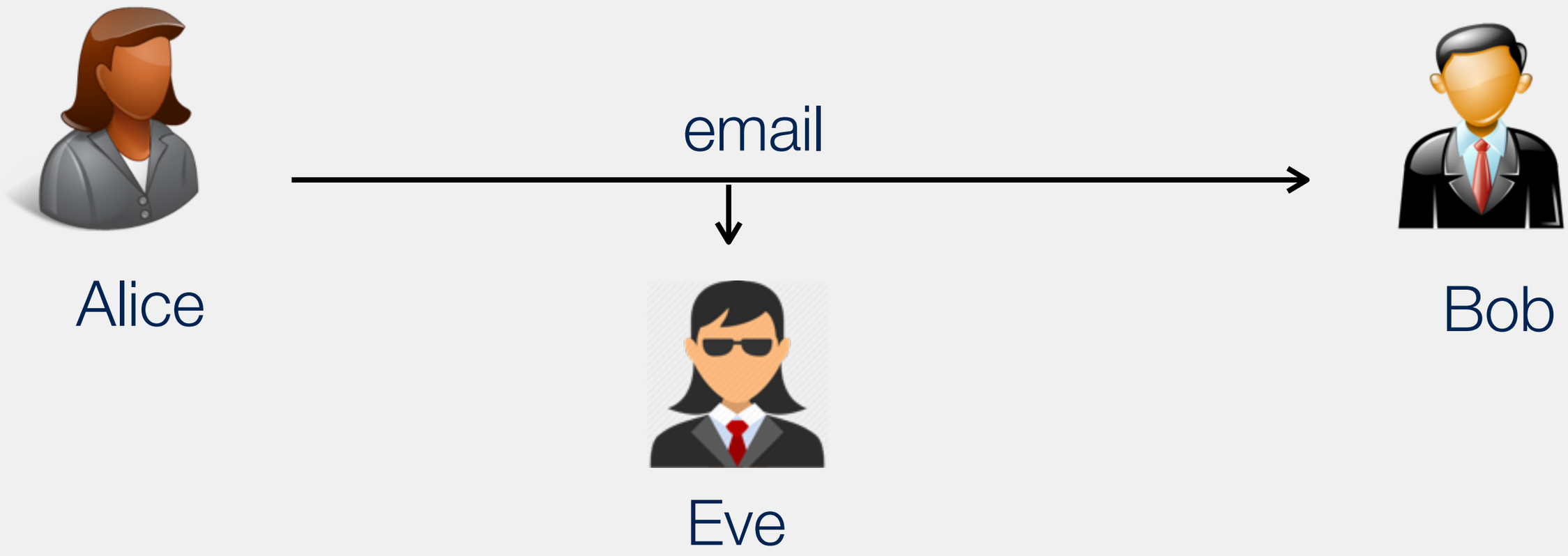
F^{-1}_{sk}: X→X

Common trapdoors permutations:

- RSA permutation
  - Based on hardness of factoring integers
- Diffie-Hellman
  - Based on the discrete logarithm problem

trapdoors

INTERMISSION



* Security goals?
  / Confidentiality, integrity, authenticity

* Symmetric encryption: fast, hard to distribute keys

* Public key encryption: slow, easy to distribute public keys

hybrid encryption

Alice

pk_A, sk_A

pk_B

$F(pk_B, x)$, $E_x(M)$

Eve

Mallory

Bob

pk_B, sk_B

pk_A

random key for this message

$x \leftarrow\$ \{0,1\}^k$

$F(pk_B, x)$, $E_x(M)$

Authenticated encryption scheme

Encrypt under Bob's pubkey

hybrid encryption

* Hash functions, HMAC

* Authenticated encryption
  / Encrypt-then-MAC
  / AES-GCM and others

* Public Key Crypto
  / Hybrid encryption
  / Digital signatures
  / Certificates, problems

* Exit slips
  / 1 thing you learned
  / 1 thing you didn't understand

recap