601.445/601.645 Practical Cryptographic Systems

Symmetric Cryptography (Cont'd)

Instructor: Matthew Green

Housekeeping

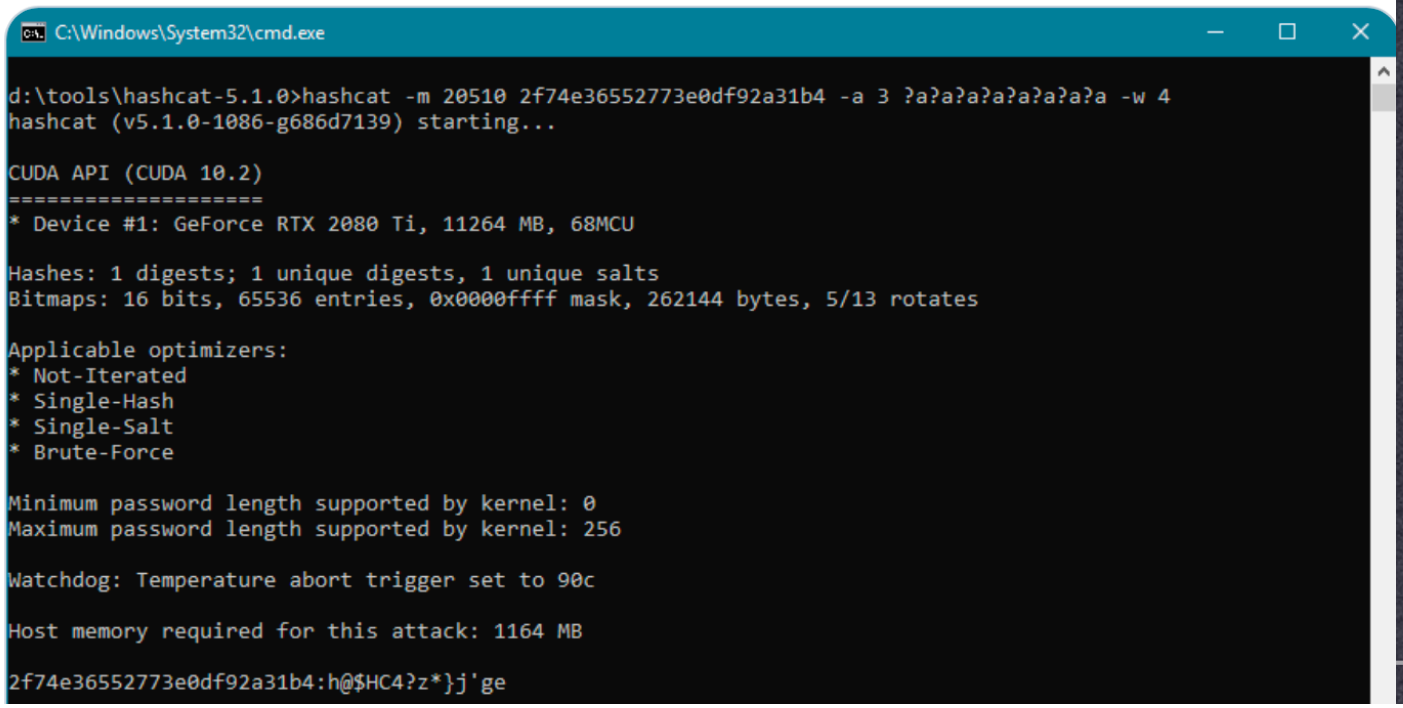
- Programming Assignment 1 Feb 13
- Written HW out today after class
- Office hours Weds after class (2-4) and TA office hours on Piazza

News?

News?

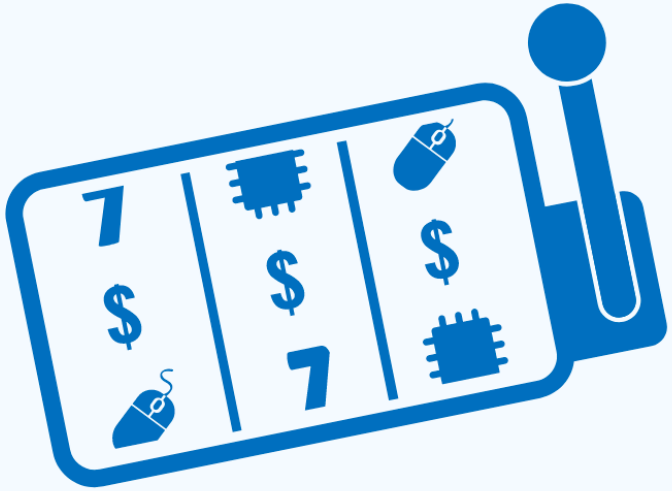
hashcat
@hashcat

Support for PKZIP Master Key added to #hashcat with an insane guessing rate of 22.7 ZettaHash/s on a single RTX 2080Ti. All passwords up to length 15 in less than 15 hours with only 4 GPUs! Excellent contribution from @s3inlc and @EU_ScienceHub bit.ly/2Q83mAM



Microsoft patches severe Windows flaw after tip-off from NSA

The US intelligence agency expects attackers to waste no time in developing tools aimed at exploiting the vulnerability



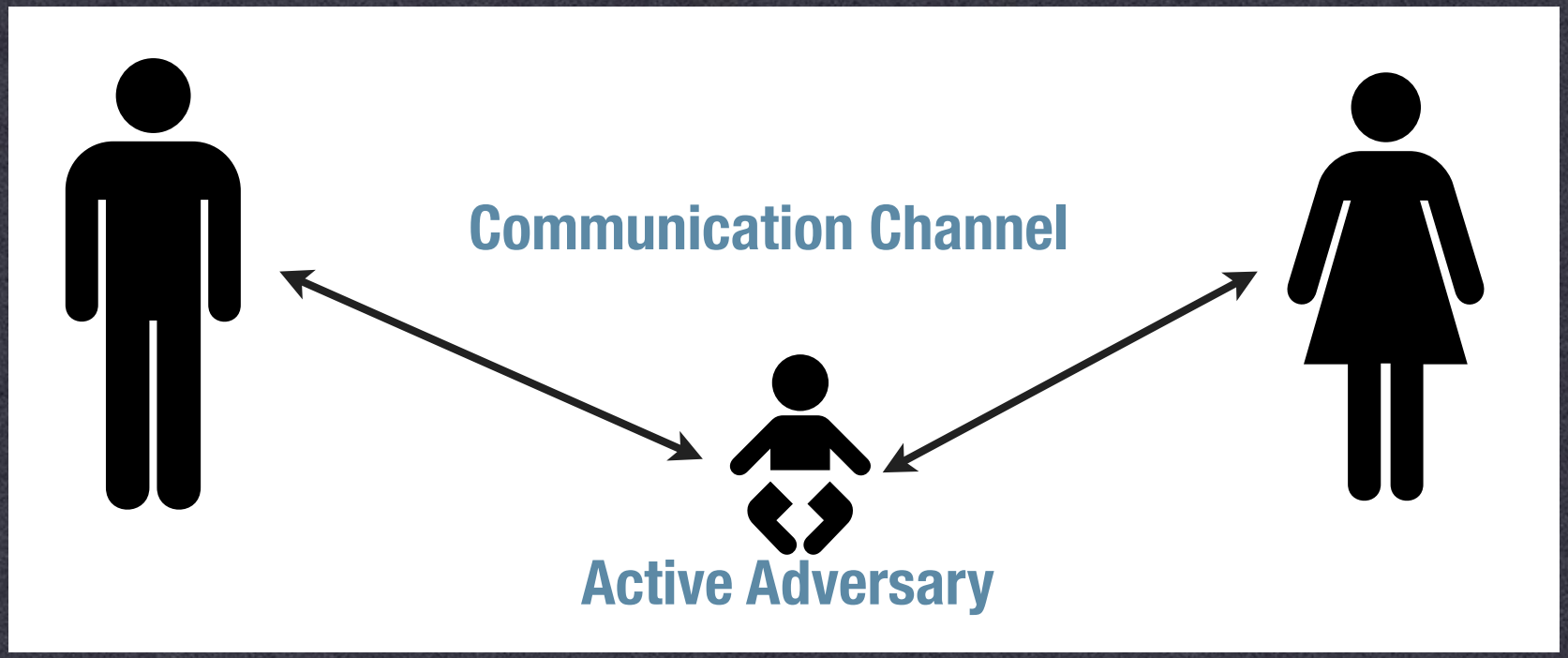
CacheOut

Leaking Data on Intel CPUs via Cache Evictions

Malleability

- The ability to modify a ciphertext
  - Such that the plaintext is meaningfully altered
  - CTR Mode (bad)
  - CBC Mode (somewhat bad)

Authenticated Encryption



MACs

- Symmetric-key primitive
  - Given a key and a message, compute a “tag”
  - Tag can be verified using the same key
  - Any changes to the message detectable
- To prevent malleability:
  - Encrypt then MAC
  - Under separate keys

MACs

- Definitions of Security
  - Existential Unforgeability under Chosen Message Attack (EU-CMA)
- Examples:
  - HMAC (based on hash functions)
  - CMAC/CBC-MAC (block ciphers)

Authenticated Encryption

- Two ways to get there:
  - Generic composition
    Encrypt (e.g., CBC mode) then MAC

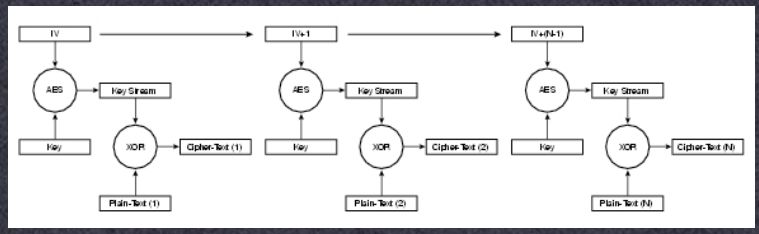
-two different keys, multiple primitives

  - Authenticated mode of operation

-Integrates both encryption & authentication

-Single key, typically uses only one primitive (e.g., block cipher)

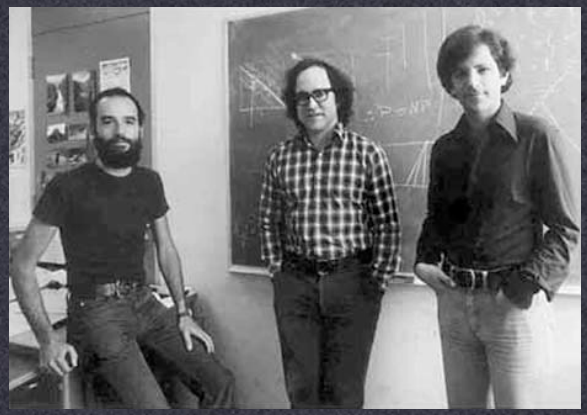
-Ex: CCM, OCB, GCM modes



How do we use encryption + MAC?

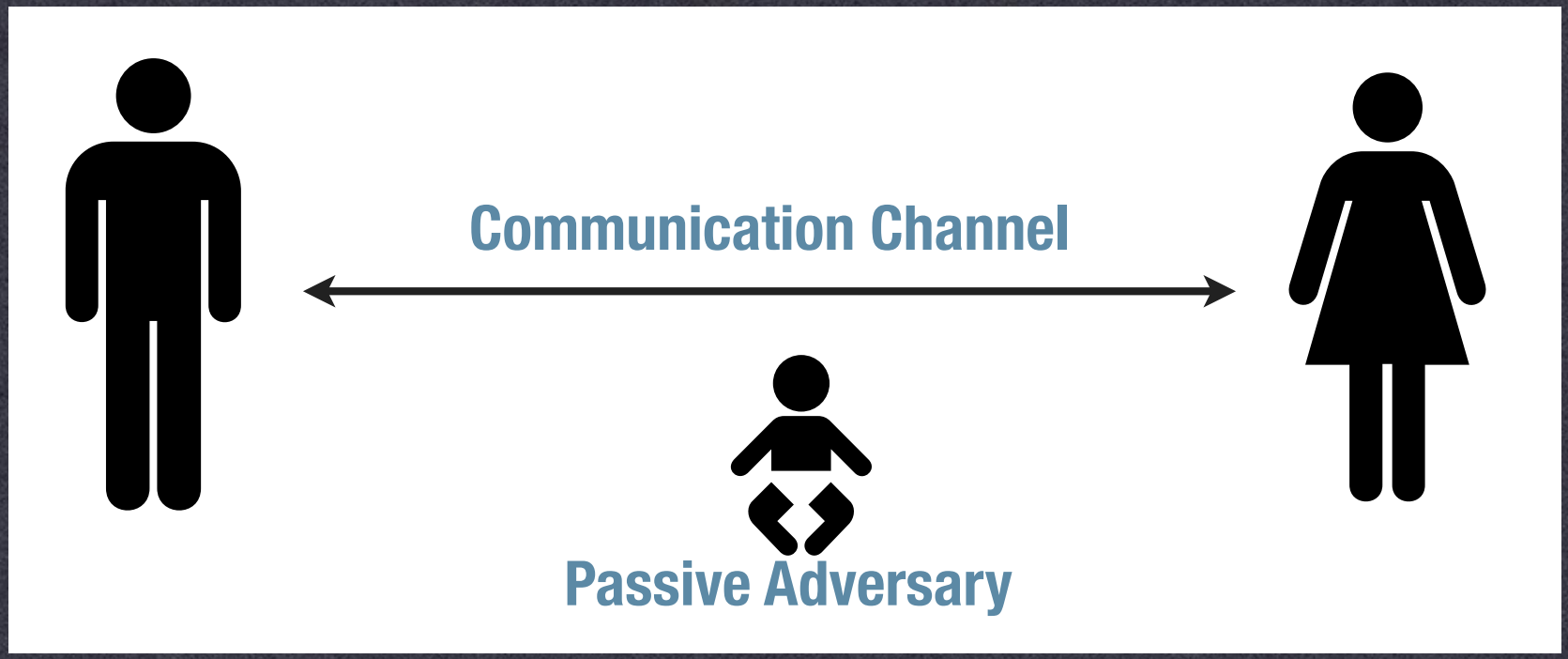
Asymmetric Crypto

- So far we've discussed symmetric crypto
  - Requires both parties to share a key
  - Key distribution is a hard problem!



Key Agreement

- Establish a shared key in the presence of a passive adversary



Abelian Groups

- G is a set of elements (e.g., integers)
  - Number of elements is “order” of group
- Plus a “group operation” (*):
  - Closure: For all a, b: a*b is in G
  - Associativity: For all a, b, c: (a*b)*c = a*(b*c)
  - Identity: Exists an element I, for all a: I*a = a*I = a
  - Inverses: For all a in G, exists b: a*b=b*a=I
  - Commutative: a*b = b*a

Cyclic Groups

- Abelian group G in which there is a generator
- A single element of G such that:
  - g, g*g, …., g^{order(G)} "generates" every element of the group
- Mathematical problems:
  - Discrete Log Problem
  - Diffie-Hellman Problem

D-H Protocol

Malcolm Williamson in 72

Diffie-Hellman in 76

$b \in \mathbb{Z}_q$ $\quad p, q : p = 2q + 1$ $\quad a \in \mathbb{Z}_q$

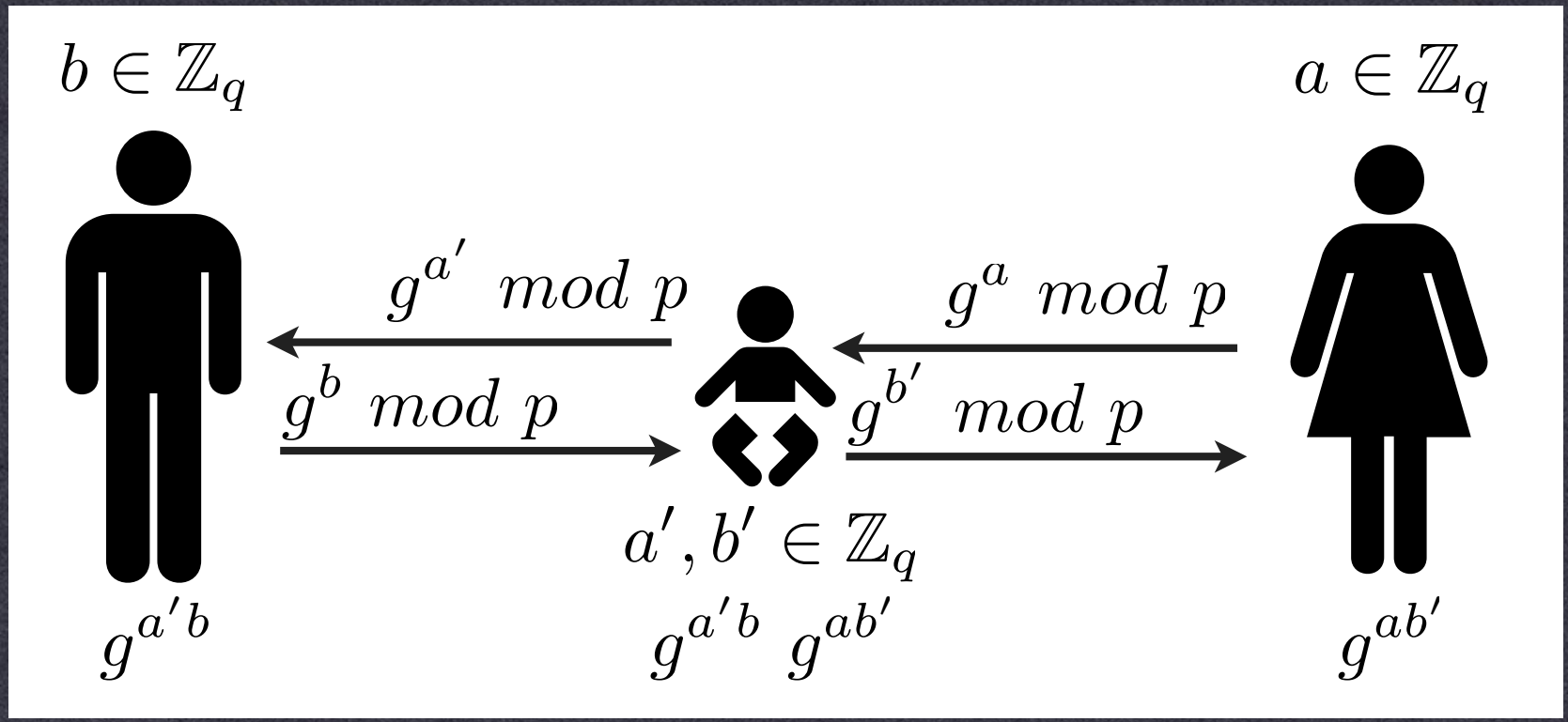
$g^a \ mod \ p$

$g^b \ mod \ p$

g^{ab} $\quad$ g^{ab}

Man in the Middle

- **Assume an <u>active</u> adversary:**



Man in the Middle

- Caused by lack of authentication
  - D-H lets us establish a shared key with anyone...
    but that's the problem...
- Solution: Authenticate the remote party

Preventing MITM

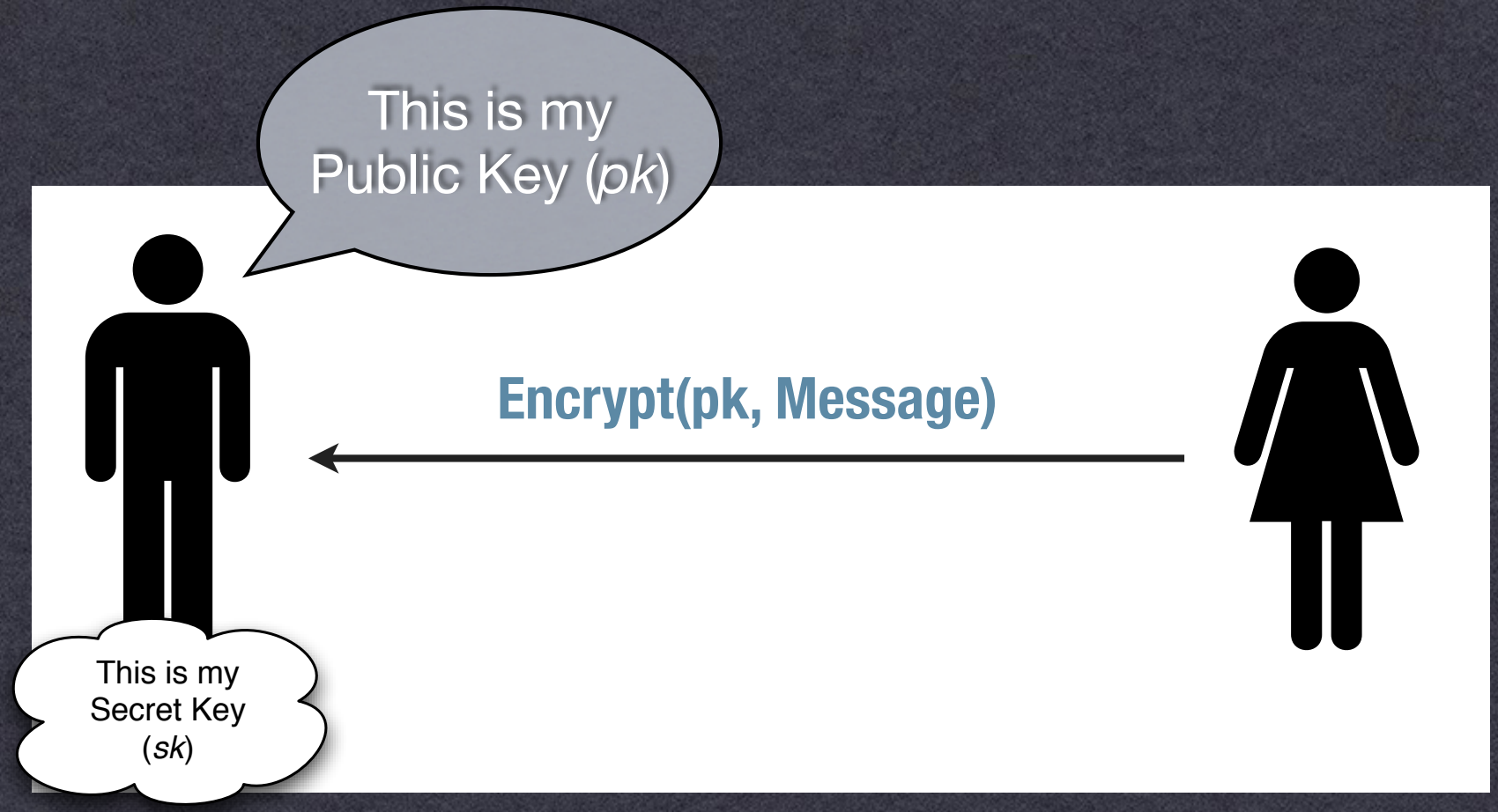
- Verify key via separate channel
- Password-based authentication
- Authentication via PKI

Public Key Encryption

- What if our recipient is <u>offline?</u>
  - Key agreement protocols are interac
  - e.g., want to send an email

Ellis in 72, Cocks a few months later

Public Key Encryption



RSA Cryptosystem

Key Generation

Choose large primes: p, q

$$N = p \cdot q$$

$$\phi(N) = (p-1)(q-1)$$

Choose:

$$e \ : \ gcd\,(e, \phi(N)) = 1$$

$$d \ : \ ed \ mod \ \phi(N) = 1$$

Output:

$$pk = (e, N)$$

$$sk = d$$

Encryption

$$c = m^e \ mod \ N$$

Decryption

$$m = c^d \ mod \ N$$

“Textbook RSA”

- In practice, we don’t use Textbook RSA
  - Fully deterministic (not semantically secure)
  - Malleable

$$c' = c \cdot x^e \ mod \ N$$

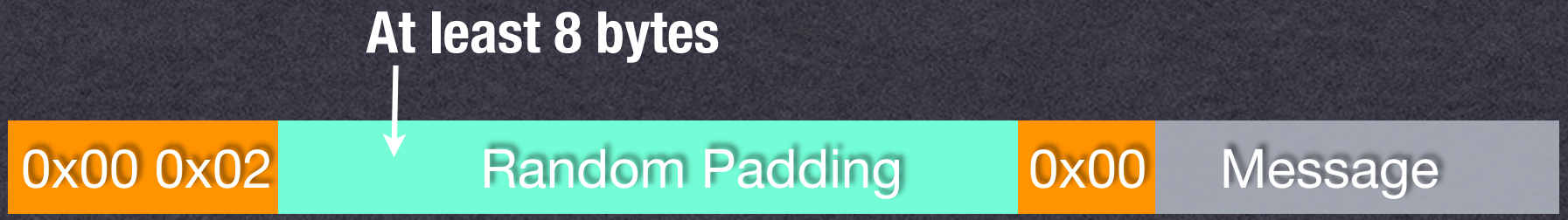
$$c'^d = (m^e \cdot x^e)^d = m \cdot x \ mod \ N$$

  - Might be partially invertible

-Coppersmith’s attack: recover part of plaintext (when m and e are small)

RSA Padding

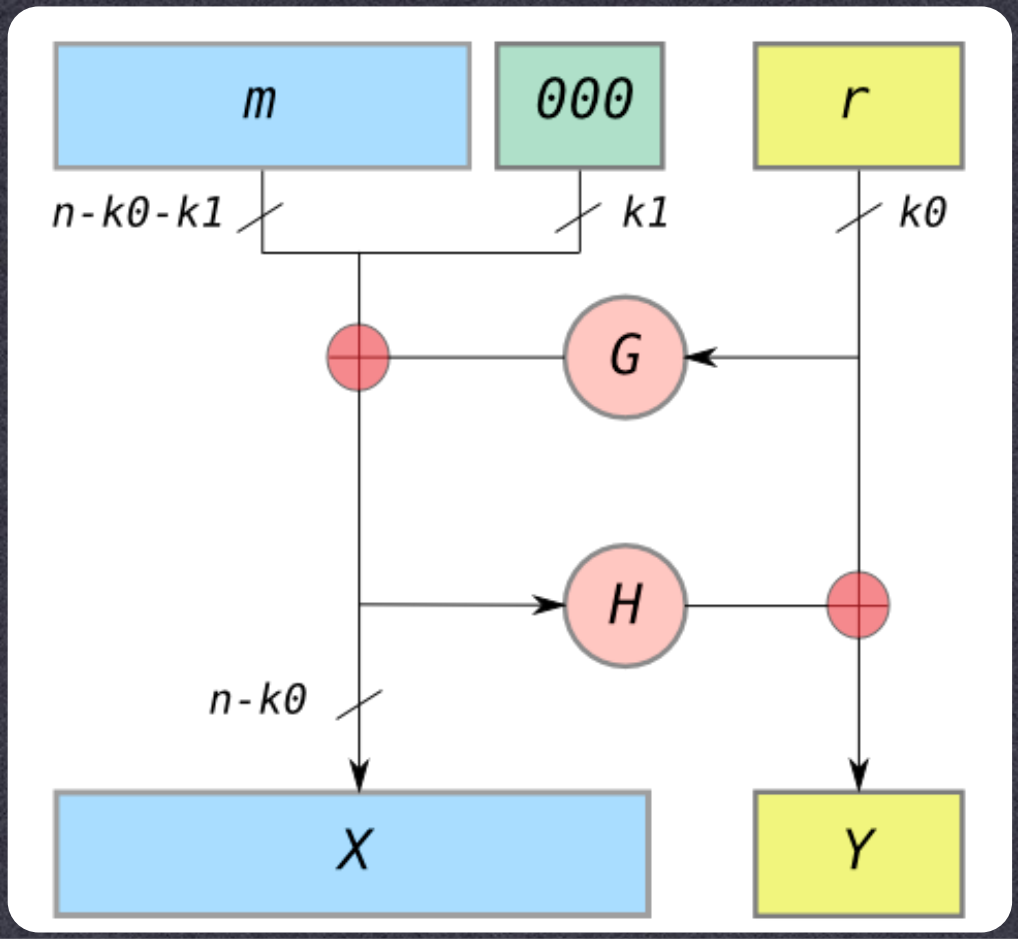
- Early solution (RSA PKCS #1 v1.5):
  - Add “padding” to the message before encryption
  - Includes randomness
  - Defined structure to mitigate malleability
  - PKCS #1 v1.5 badly broken (Bleichenbacher)



~ 1024 bits (128 bytes)

RSA Padding

- Better solution (RSA-OAEP):
  - G and H are hash functions



Efficiency

	Cycles/Byte
AES (128 bit key)	18
DES (56 bit key)	51
RSA (1024 bit key) Encryption	1,016
RSA (1024 bit key) Decryption	21,719

$m^e \ mod \ N$
$e = 65,537$

$m^d \ mod \ N$

Benchmarks from: http://www.cryptopp.com/benchmarks.html
Microsoft Visual C++, Windows XP, Intel Core 2 1.83Mhz in 32-bit mode

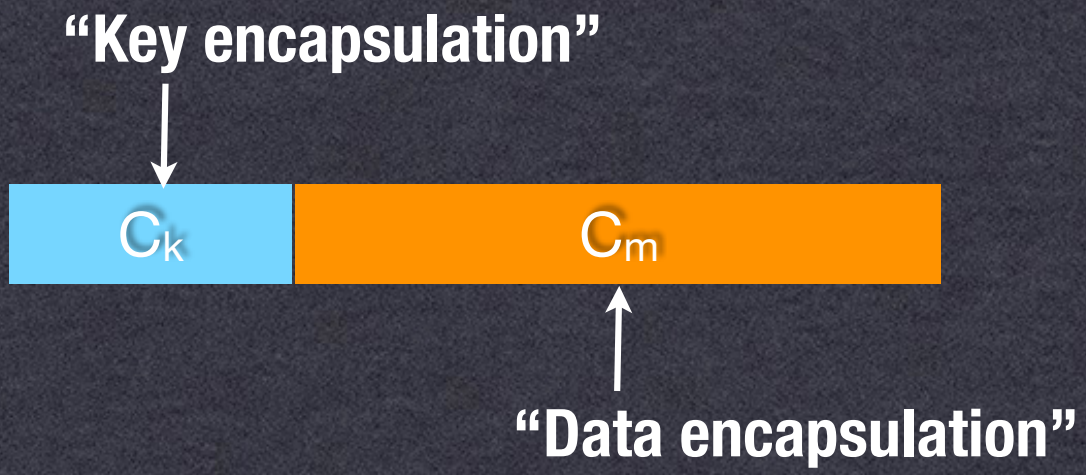
Hybrid Encryption

- **Mixed Approach**
  - **Use PK encryption to encrypt a symmetric key**
  - **Use (fast) symmetric encryption on data**

$$k \xleftarrow{\$} \{0,1\}^k$$

$$C_k \leftarrow RSA.Encrypt_{pk}(k)$$

$$C_m \leftarrow AES.Encrypt_k(message)$$



Key Strength

Level	Protection	Symmetric	Asymmetric	Discrete Logarithm Key	Discrete Logarithm Group	Elliptic Curve	Hash
1	Attacks in "real-time" by individuals *Only acceptable for authentication tag size*	32	-	-	-	-	-
2	Very short-term protection against small organizations *Should not be used for confidentiality in new systems*	64	816	128	816	128	128
3	Short-term protection against medium organizations, medium-term protection against small organizations	72	1008	144	1008	144	144
4	Very short-term protection against agencies, long-term protection against small organizations *Smallest general-purpose level,* *Use of 2-key 3DES restricted to 2^{40} plaintext/ciphertexts,* *protection from 2009 to 2011*	80	1248	160	1248	160	160
5	Legacy standard level *Use of 2-key 3DES restricted to 10^6 plaintext/ciphertexts,* *protection from 2009 to 2018*	96	1776	192	1776	192	192
6	Medium-term protection *Use of 3-key 3DES,* *protection from 2009 to 2028*	112	2432	224	2432	224	224
7	Long-term protection *Generic application-independent recommendation,* *protection from 2009 to 2038*	128	3248	256	3248	256	256
8	"Foreseeable future" *Good protection against quantum computers*	256	15424	512	15424	512	512

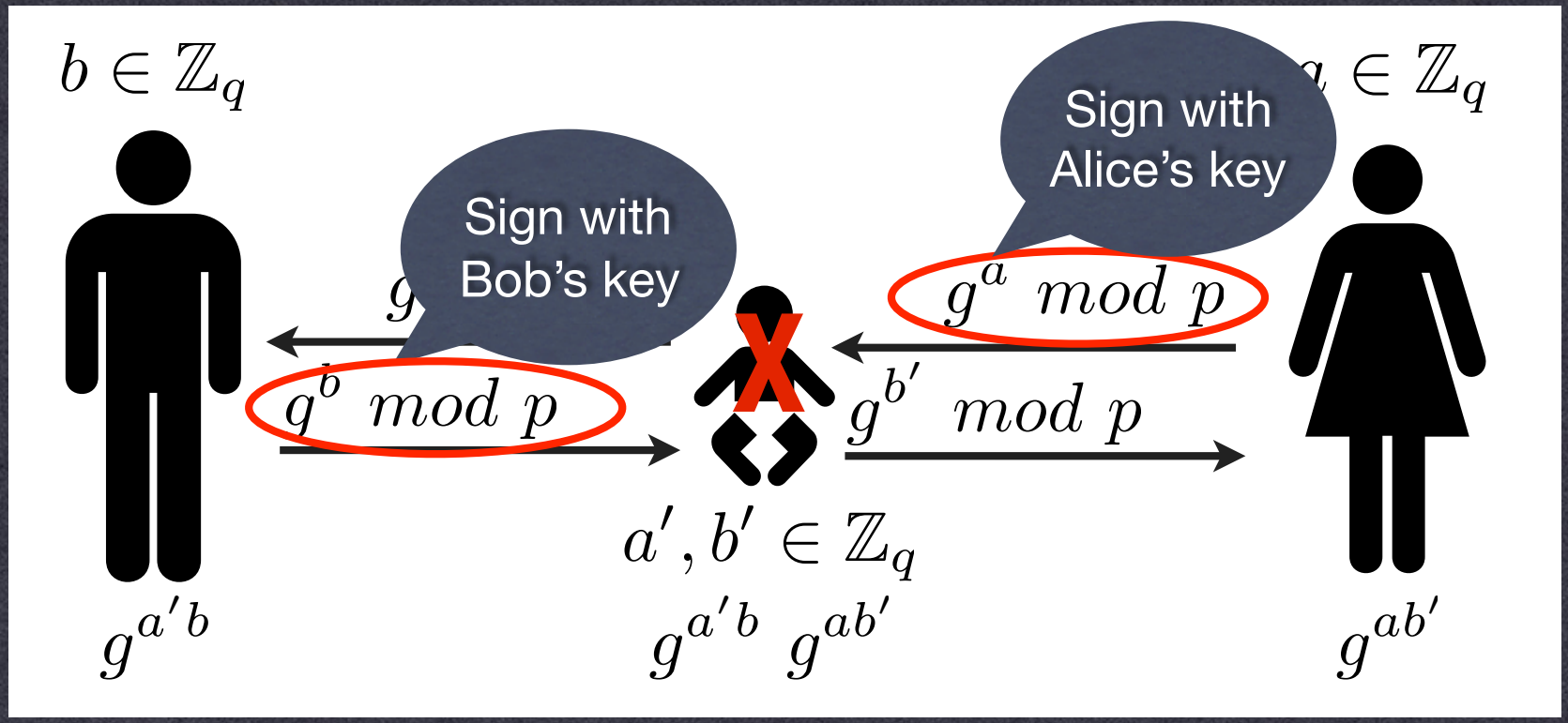
Source: www.keystrength.com (BlueKrypt). Based on ECrypt recommendations.

Digital Signatures

- Similar to MACs, with public keys
  - Secret key used to sign data
  - Public key can verify signature
  - Advantages over MACs?

Preventing MitM

- **Assume an <u>active</u> adversary:**



PKI & Certificates

- How do I know to trust your public key?
  - Put it into a file with some other info, and get someone else to sign it!

Next Time

- Protocols & Implementation
- Reading!
- A2 coming up this week