Practical Cryptographic Systems

Symmetric Cryptography II & Asymmetric Cryptography

Instructor: Matthew Green

Housekeeping

- A2 (part 1) due tonight
- A2 (part 2) out now
- New reading: attacks on RSA paper
  - Dan Boneh
- Late day policy update (A2 and beyond):
  - 3 total late days to be used at discretion
  - Please note these on your assignment!
  - 25% per day late after that

Housekeeping

- Projects
    - I will put up a tentative list on Github and we'll talk Weds about this

News

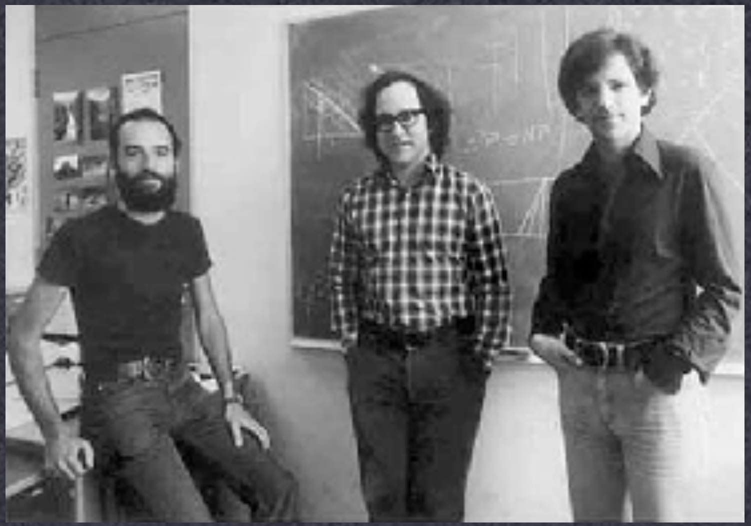
Review

- Last time:
  - Padding oracles
  - Introduction to algebraic groups
  - Diffie-Hellman (MITM)

Hash Functions

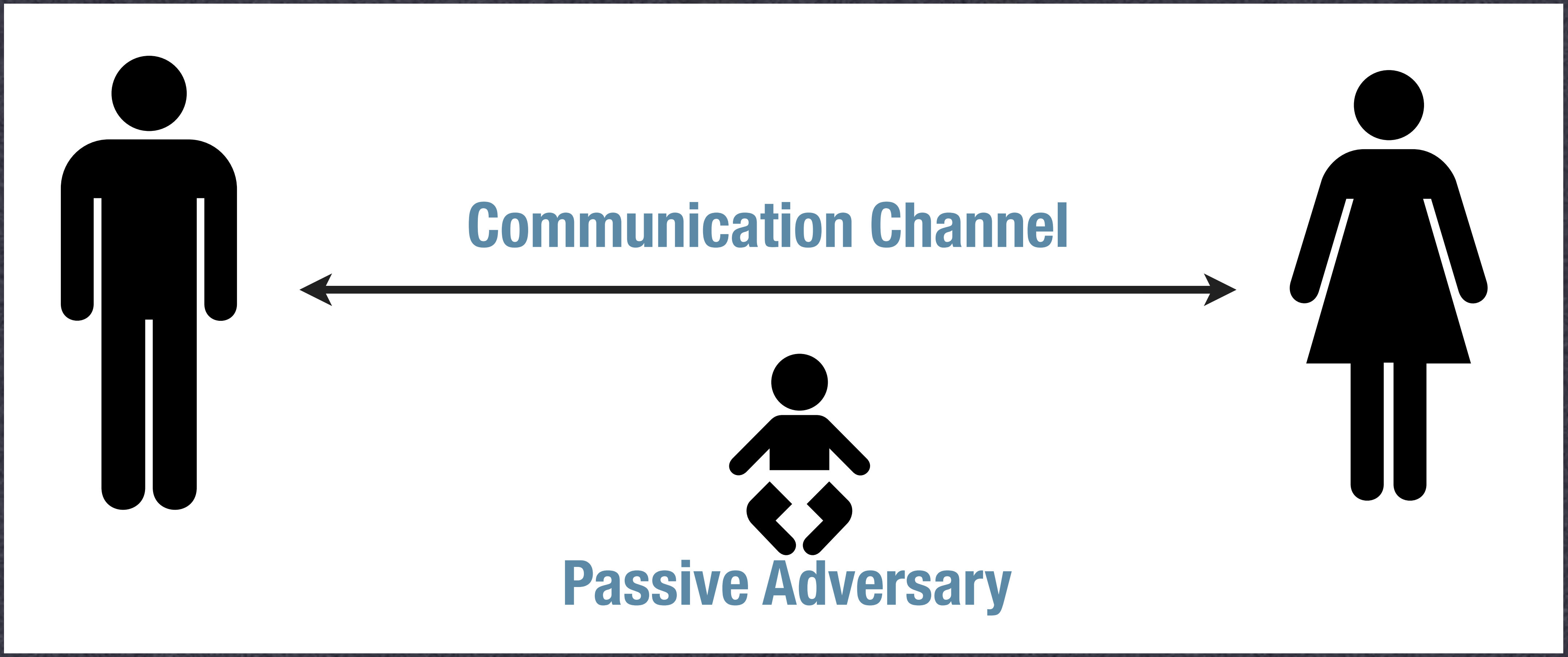
Asymmetric Crypto

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



Key Agreement

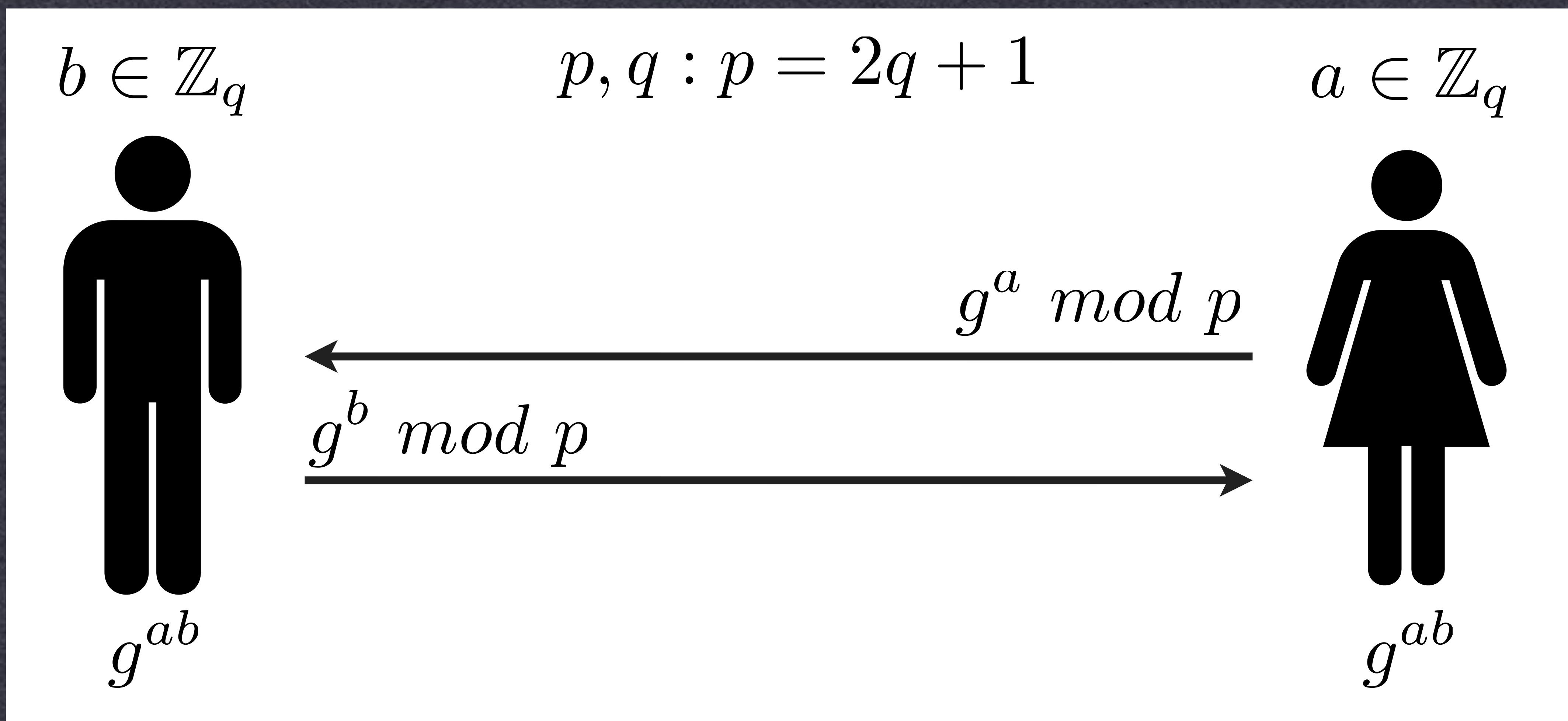
- Establish a shared key in the presence of a passive adversary



D-H Protocol

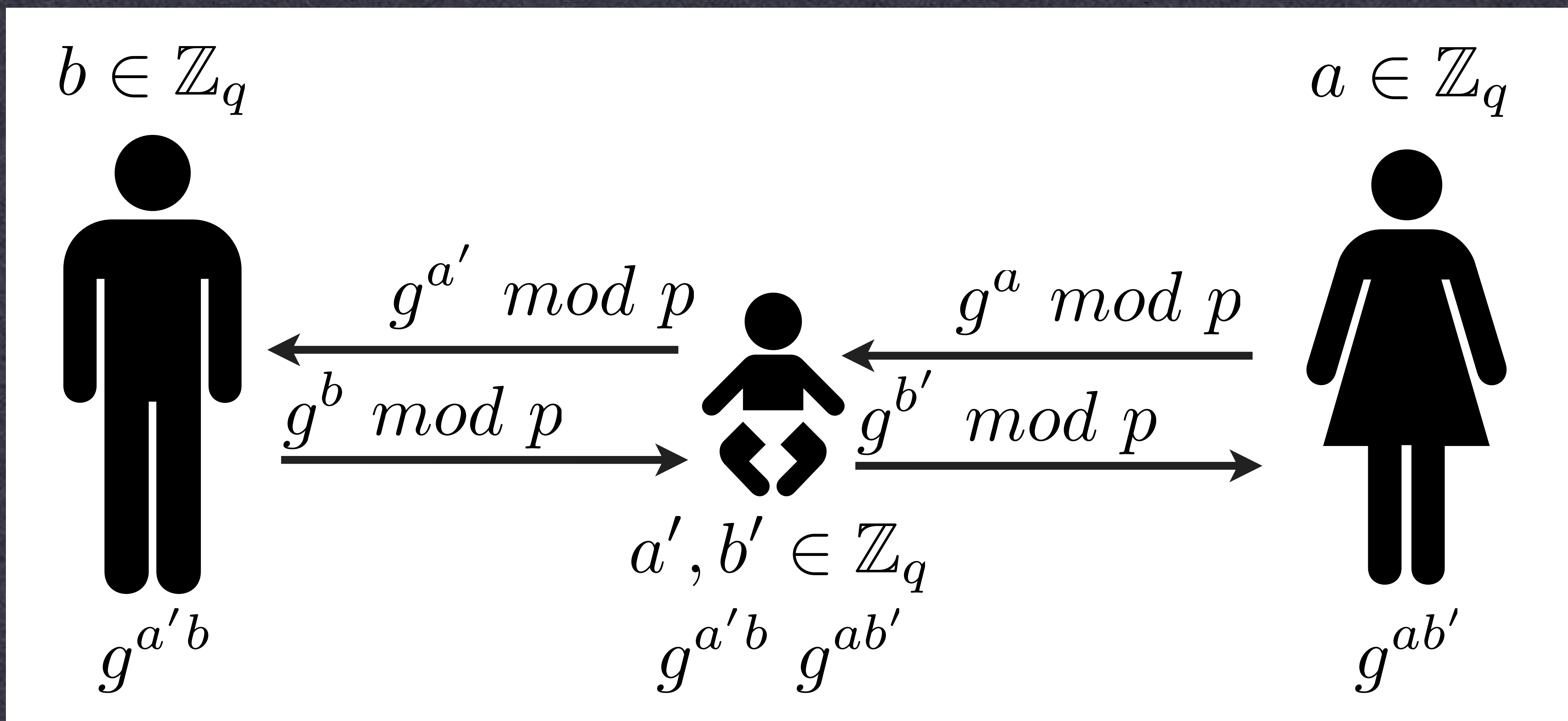
Malcolm Williamson in 72

Diffie-Hellman in 76



Man in the Middle

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



Man in the Middle

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

Preventing MITM

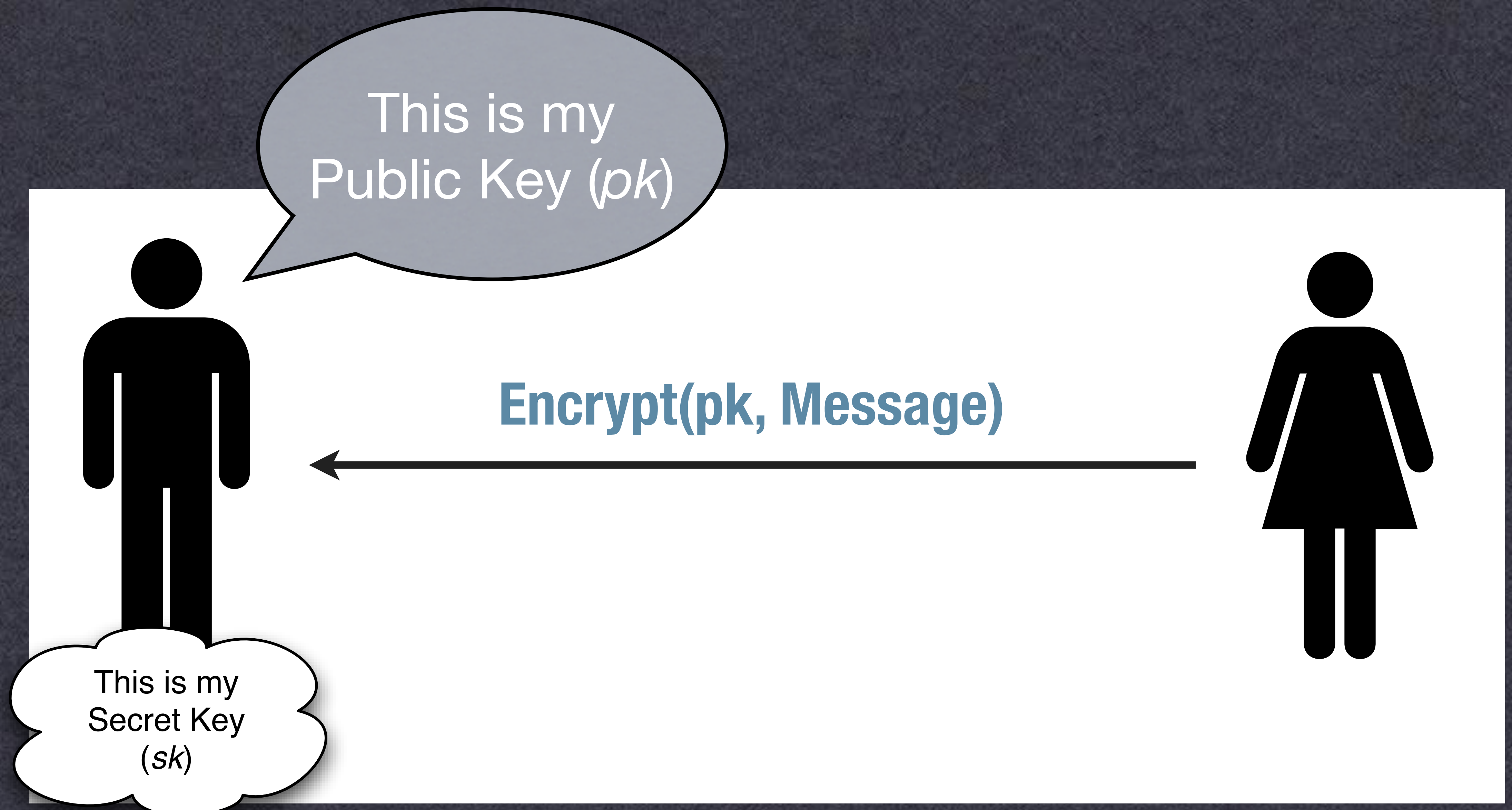
- Verify key via separate channel
- Password-based authentication
- Authentication via PKI

Public Key Encryption

Ellis in 72, Cocks a few months later

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

Public Key Encryption



RSA Cryptosystem

Key Generation

Choose large primes: p, q

$$N = p \cdot q$$

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

Choose:

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

$$d \text{ : } ed \; mod \; \phi(N) = 1$$

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

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

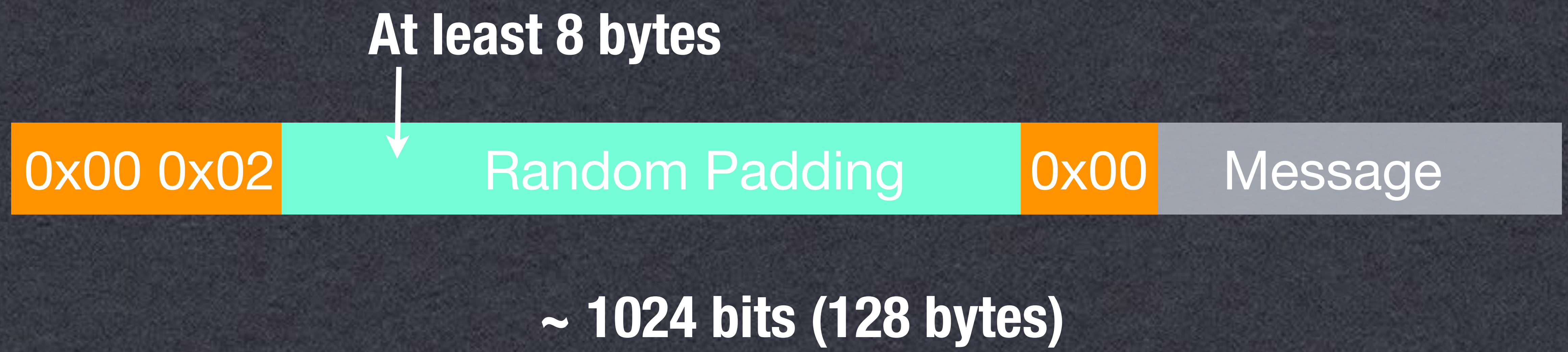
$$c'^d = (m^e \cdot x^e)^d = m \cdot x \ mod \ N$$

  - Might be partially invertible

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

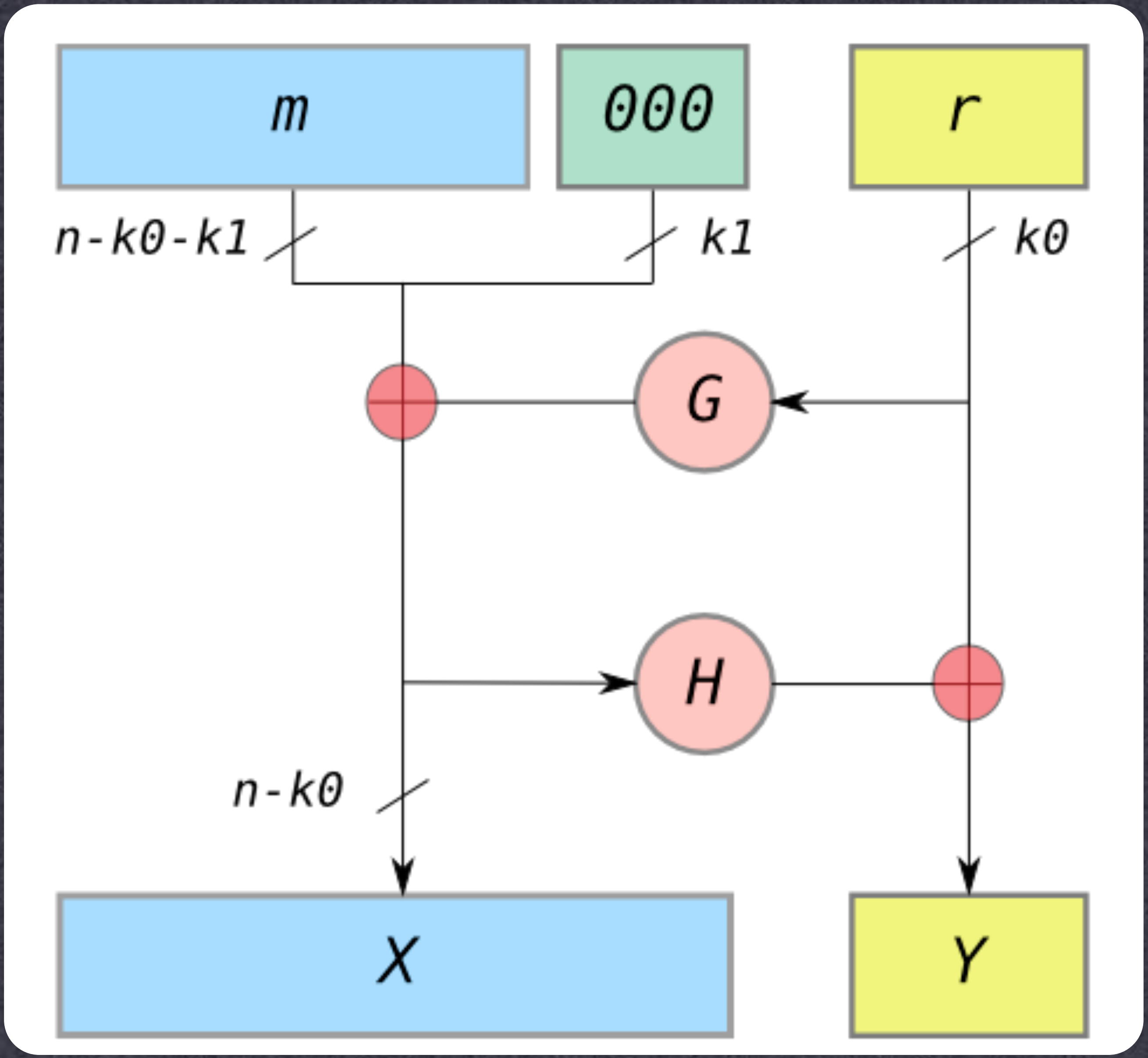
RSA Padding

- 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)



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) <u>Encryption</u>	1,016
RSA (1024 bit key) <u>Decryption</u>	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

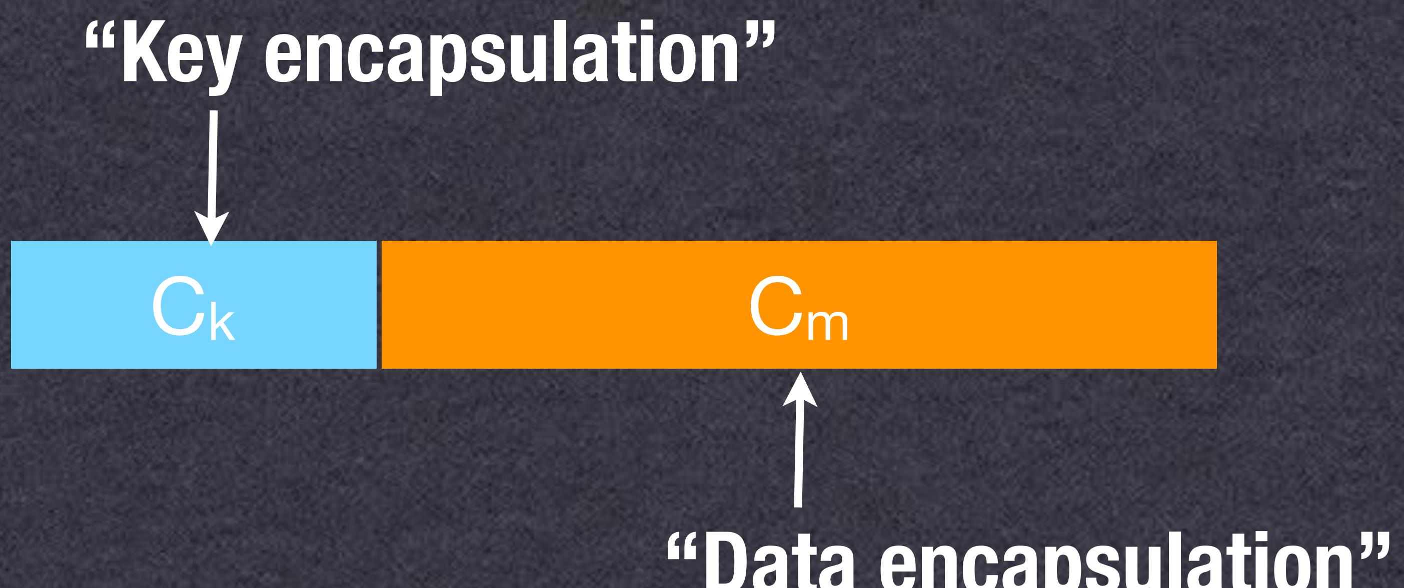
Hybrid Encryption

- **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

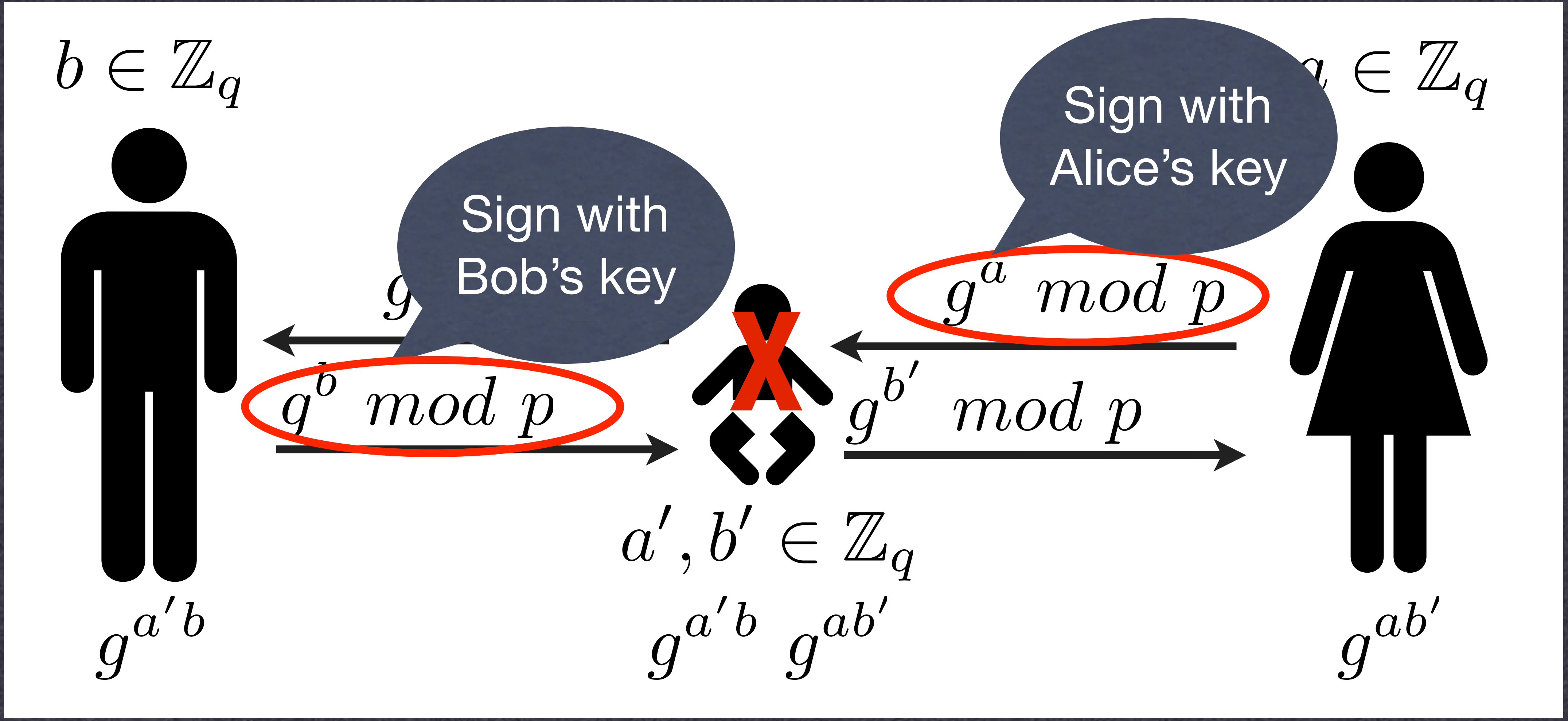
Source: www.keystrength.com (BlueKrypt). Based on ECrypt recommendations.

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 active 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