Practical Cryptographic Systems

Asymmetric Cryptography III

Instructor: Matthew Green

Housekeeping

- A2 will be out on Monday
- Reading assignment (short!) out on Weds
- TA is working on grades
  - (Reminder: we have a late-day policy, 120 hours.)

News?

Nev

Canada to Ban Flipper Zero Devices Over Car Thefts

However, Flipper Devices says the tool can't be used to unlock cars made in the last 30 years.

By Michael Kan February 9, 2024

Ne

HACKADAY

HOME BLOG HACKADAY.IO TINDIE HACKADAY PRIZE SUBMIT ABOUT February 12, 2024

CANADA BANS FLIPPER ZERO OVER WHAT IT IMAGINES IT DOES

by: Donald Papp

39 Comments

February 12, 2024

Canada to Ban Flipper Zero Devices Over

News?

- https://blog.flipper.net/rfid/

Review

- Key exchange (DH)
- Public key encryption?

Review

- How many elements are in Z*p?
  - Note: every element a in *Zp* s.t. gcd(*a, p*) = 1 has an inverse, is in Z*p
  - This is also denoted by Euler's totient function, $\phi(\cdot)$
  - For all primes p: $\phi(p) = p - 1$
  - We also refer to this as the order of the group
    (sometimes we also refer to the order of the generator *g* as *order(g).)*
- Not every element of the group is a generator

See Boneh-Shoup, Appendix A

Review

$$a, b \in \{0, 1, \ldots, p-1\} \qquad \langle g \rangle = \mathbb{Z}_p^*$$

$$g^{order(g)} = 1$$

$$g^a \cdot g^b = g^{a+b \ mod \ order(g)}$$

$$(g^a)^b = (g^b)^a = g^{a*b \ mod \ order(g)}$$

See Boneh-Shoup, Appendix A

Review: DLP

- **Discrete logarithm problem**

  Given: $x \in_R 0, \ldots, p-2$

  $$\langle g \rangle = \mathbb{G} \qquad order(g) = p - 1$$

  $$h = g^x$$

  Find: x

  This problem is hard if for all p.p.t. adversaries, all attackers find x with "small" probability

See Boneh-Shoup, Appendix A

Review: DLP

- **Discrete logarithm problem**

  Given: $x \in_R 0, \ldots, p-2$

  $\langle g \rangle = \mathbb{G}$ $order(g) = p$

  $h = g^x$

  Find: x

This means that "reversing" exponentiation is assumed to have super-polynomial running time.

How about the exponentiation itself?

Note that for this to hold, the size of *p* must be pretty large!

In practice, we typically assume *p* is at least 1024 bits. And 3072 bits is the minimum in modern protocols!

This problem is hard if for all p.p.t. adversaries, all attackers find x with "small" probability

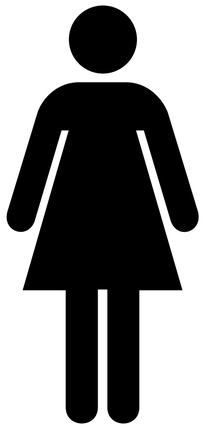
See Boneh-Shoup, Appendix A

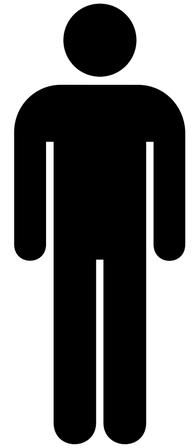
Review: D-H Protocol

$p, \langle g \rangle = \mathbb{Z}_p^*$

$a \in \mathbb{Z}_{\phi(p)}$

$b \in \mathbb{Z}_{\phi(p)}$





p, g, g^a

g^b

g^{ba}

g^{ab}

Usually we “hash” the shared secret value to make a secret encryption key, and then encrypt using a fast symmetric encryption scheme!

Review: DH problem

- **Diffie-Hellman problem**

  Given: $a, b \in_R 0, \ldots, p-2$

  $$\langle g \rangle = \mathbb{G} \qquad order(g) = p - 1$$

  $$(g, g^a, g^b)$$

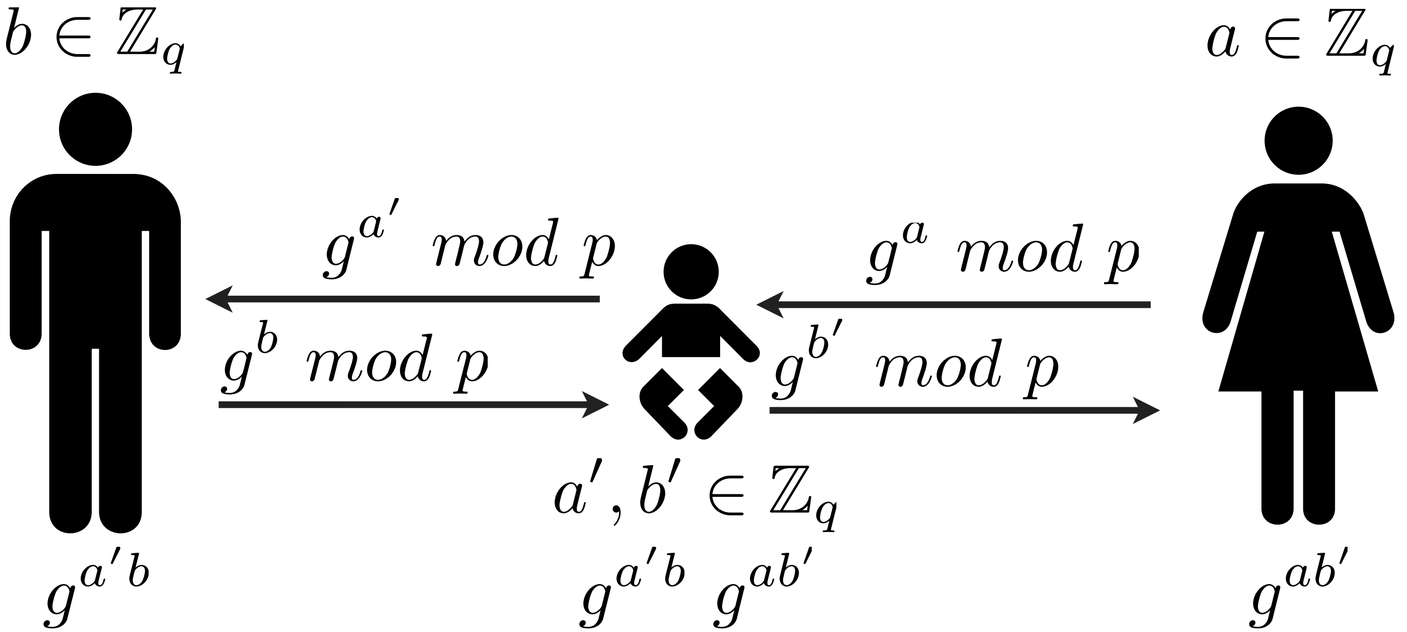
  Find: g^{ab}

  We believe this problem is hard if for all p.p.t. classical adversaries, all attackers output a solution with “small” probability

See Boneh-Shoup, Appendix A

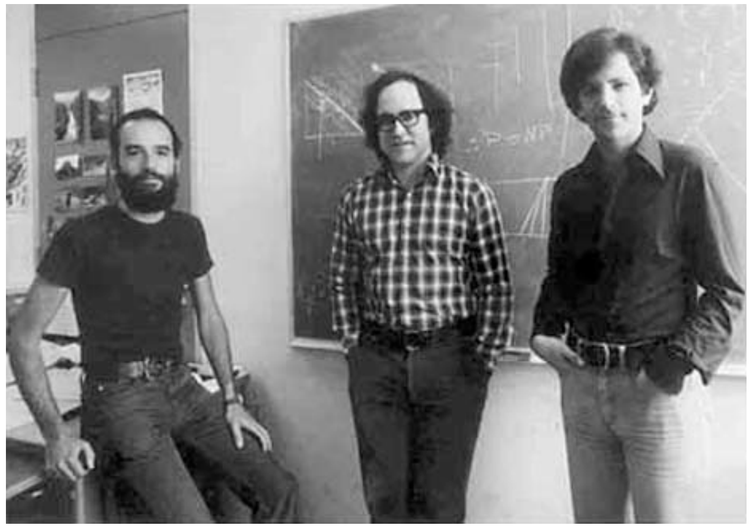
Review: MITM

- Assume an active adversary:

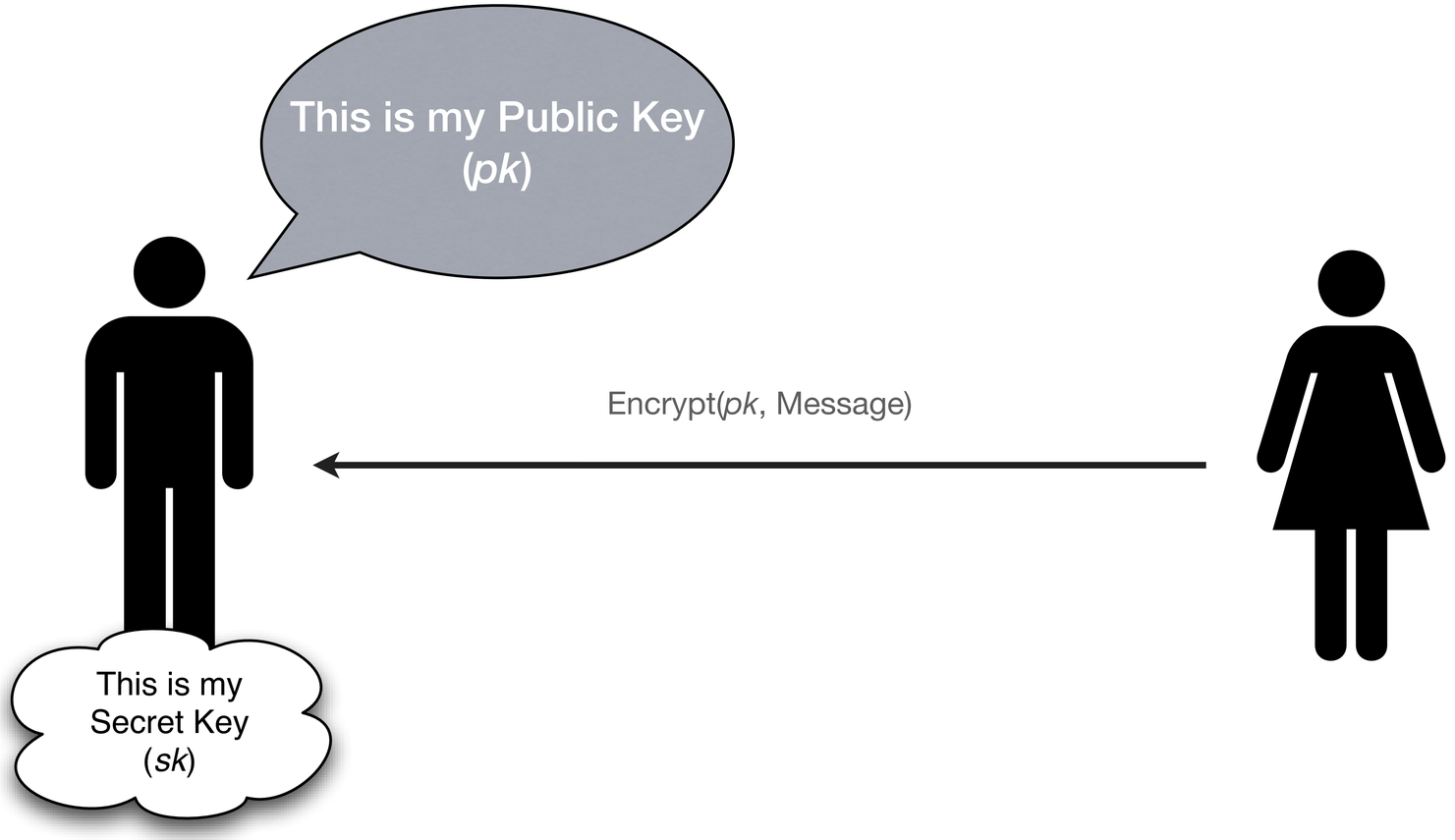


Public Key Encryption

- What if our recipient is offline?
  - Key agreement protocols are interactive
  - e.g., want to send an email



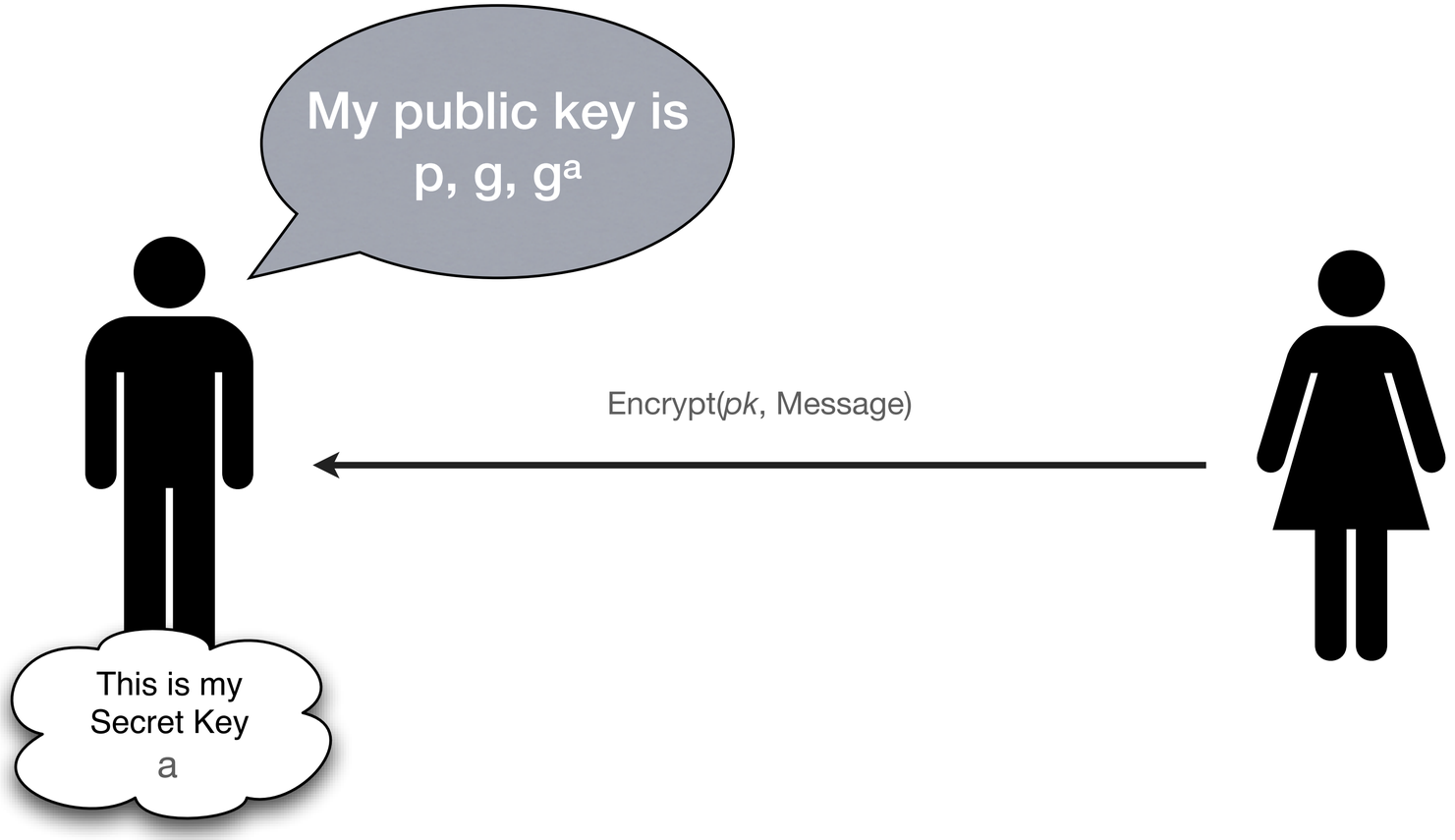
Public Key Encryption



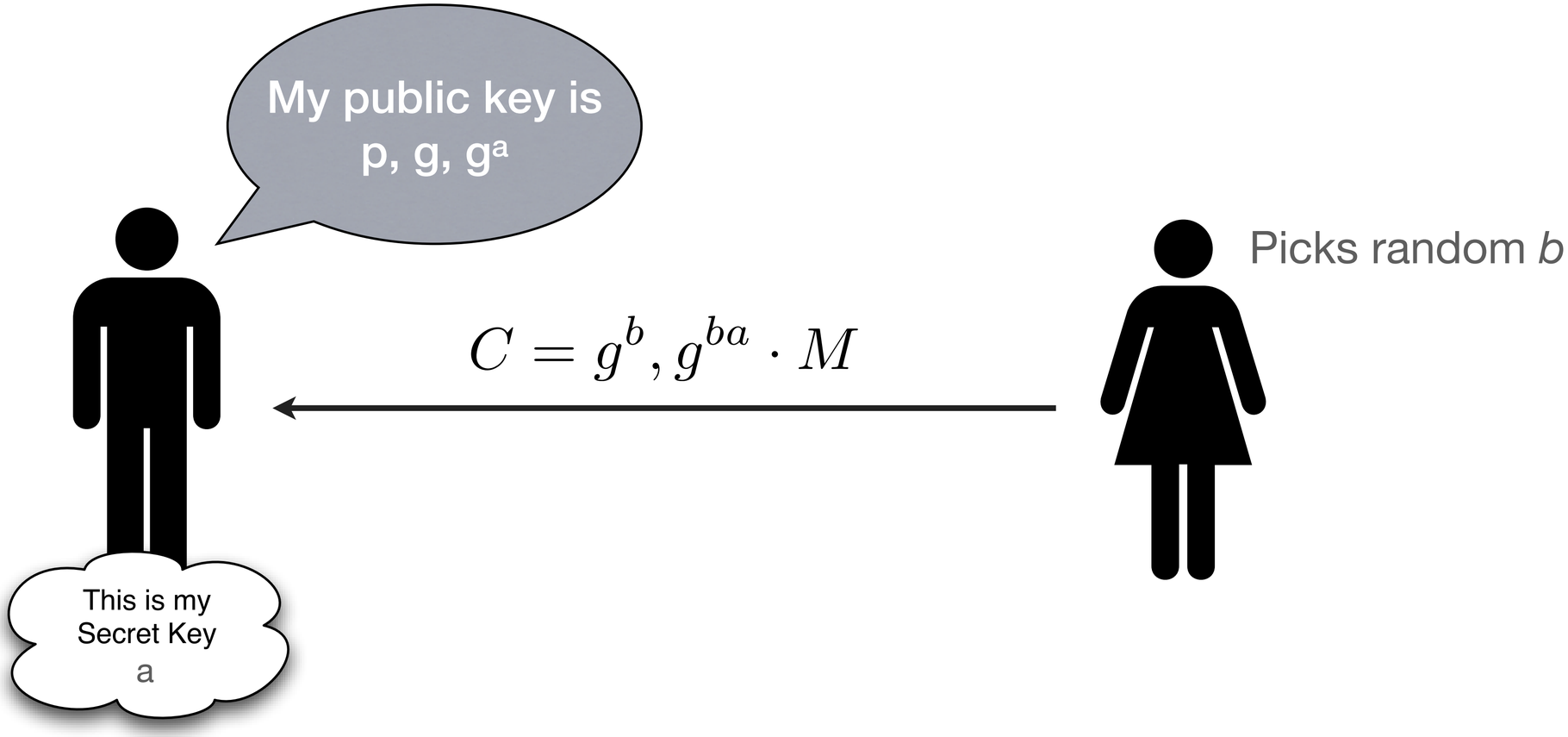
Public key encryption from D-H?

- Can we build public-key encryption from Diffie-Hellman?
- Idea: we will re-use the first move of the D-H protocol as a “public key”
  - Does this work?

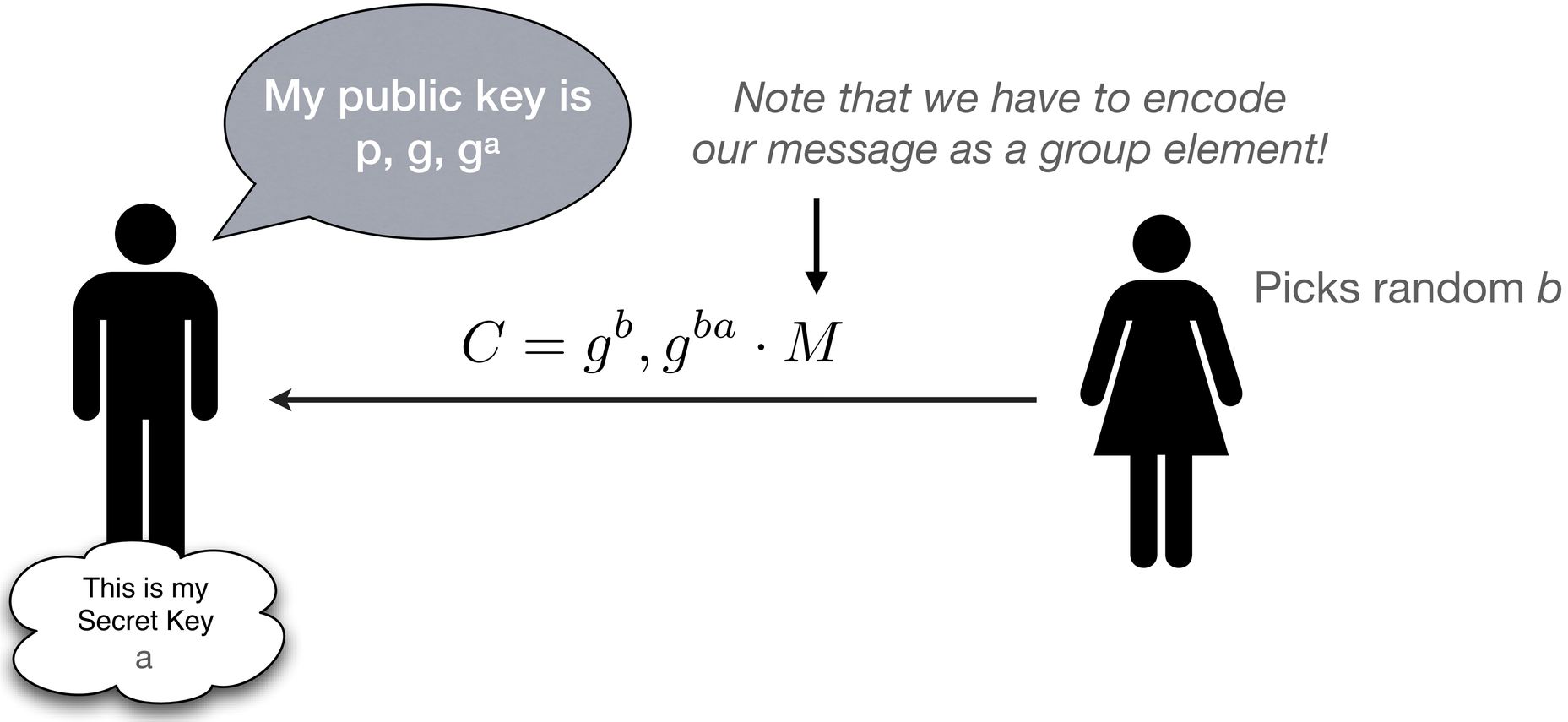
“DH for PKE” (Elgamal)



“DH for PKE” (Elgamal)



“DH for PKE” (Elgamal)



Quadratic residues & Legendre symbol

- New notion: Quadratic Residues (mod p)
  - The subgroup of quadratic residues QR_p is the set of squares modulo p: let x, y be in Z*p

    if $x = y^2$, then x is a quadratic residue

    This is the subgroup of order (p-1)/2 that always exists for $p > 2$, p prime

See Boneh-Shoup, Appendix A

Quadratic residues & Legendre symbol

- Some quick facts about quadratic residues:
  - Let x, y be quadratic residues: then so is x*y

$$g^{\text{even}} \cdot g^{\text{even}} = g^{\text{even } mod\ p-1}$$

  - If x is a *QR*, y is not a QR: x*y is not a QR

$$g^{\text{odd}} \cdot g^{\text{even}} = g^{\text{odd } mod\ p-1}$$

  - If x, y are not QR, then x*y is a QR

$$g^{\text{odd}} \cdot g^{\text{odd}} = g^{\text{even } mod\ p-1}$$

See Boneh-Shoup, Appendix A

Legendre symbol

- The Legendre symbol will tell you if x is a quadratic residue mod p:

Is 0 mod p Is a QR mod p

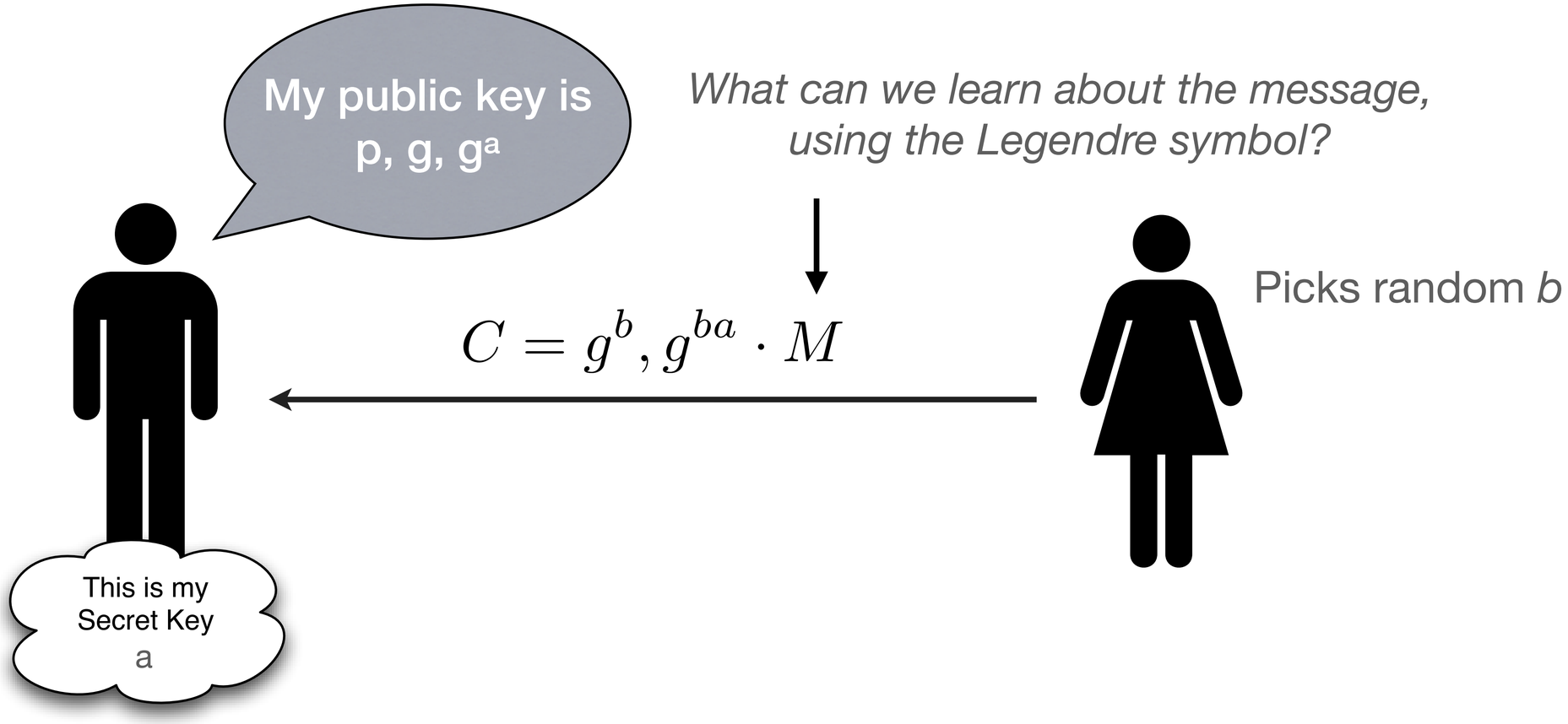
$$\left(\frac{x}{p}\right) = \{-1, 0, 1\}$$

Is not a QR mod p

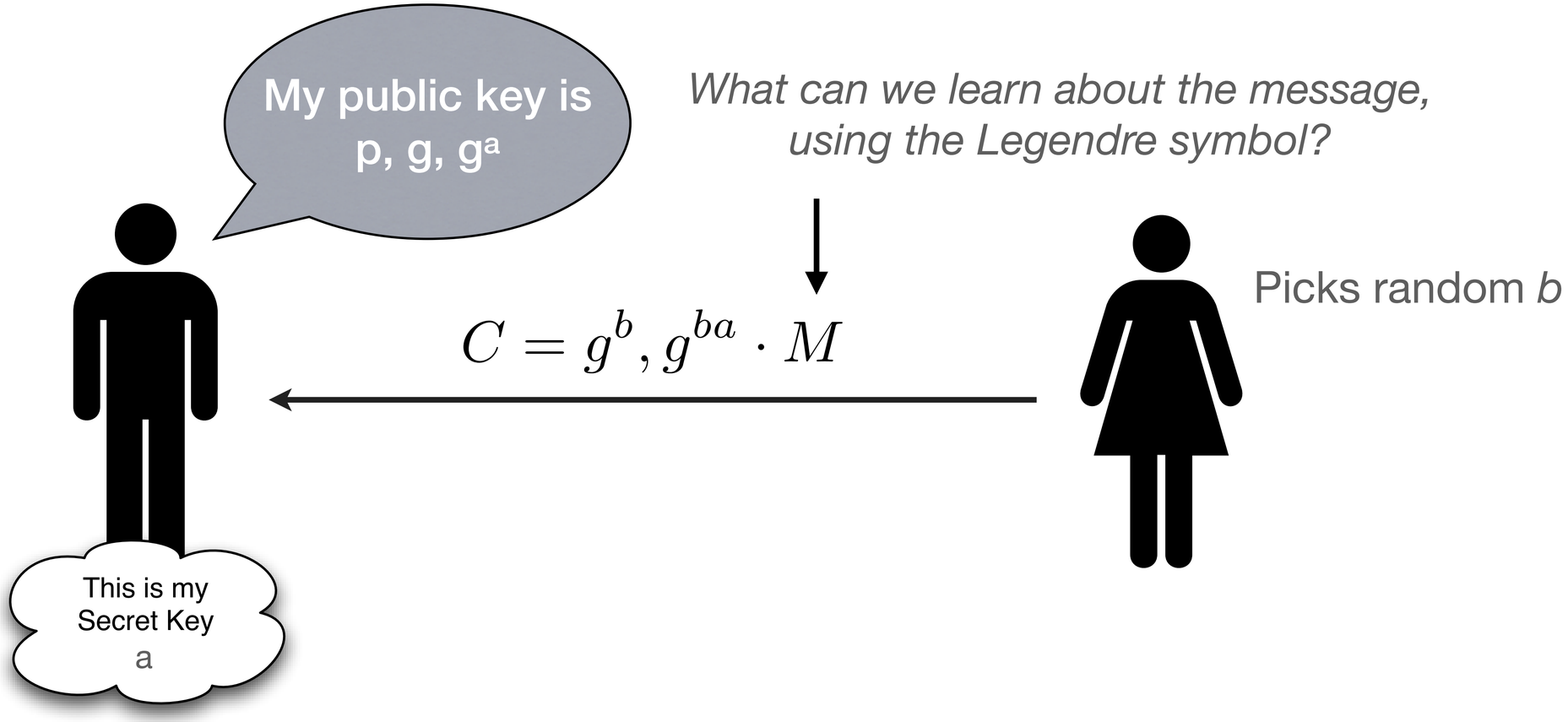
- **Euler's theorem**: x is a QR iff $x^{(p-1)/2} = 1$

See Boneh-Shoup, Appendix A

Weakness: Elgamal



How do we fix this?



How do we fix this?

- Answer #1:
  - Don’t use groups that have subgroups (of QR)!
  - Q: How do we generate a group that doesn’t have any large subgroups?

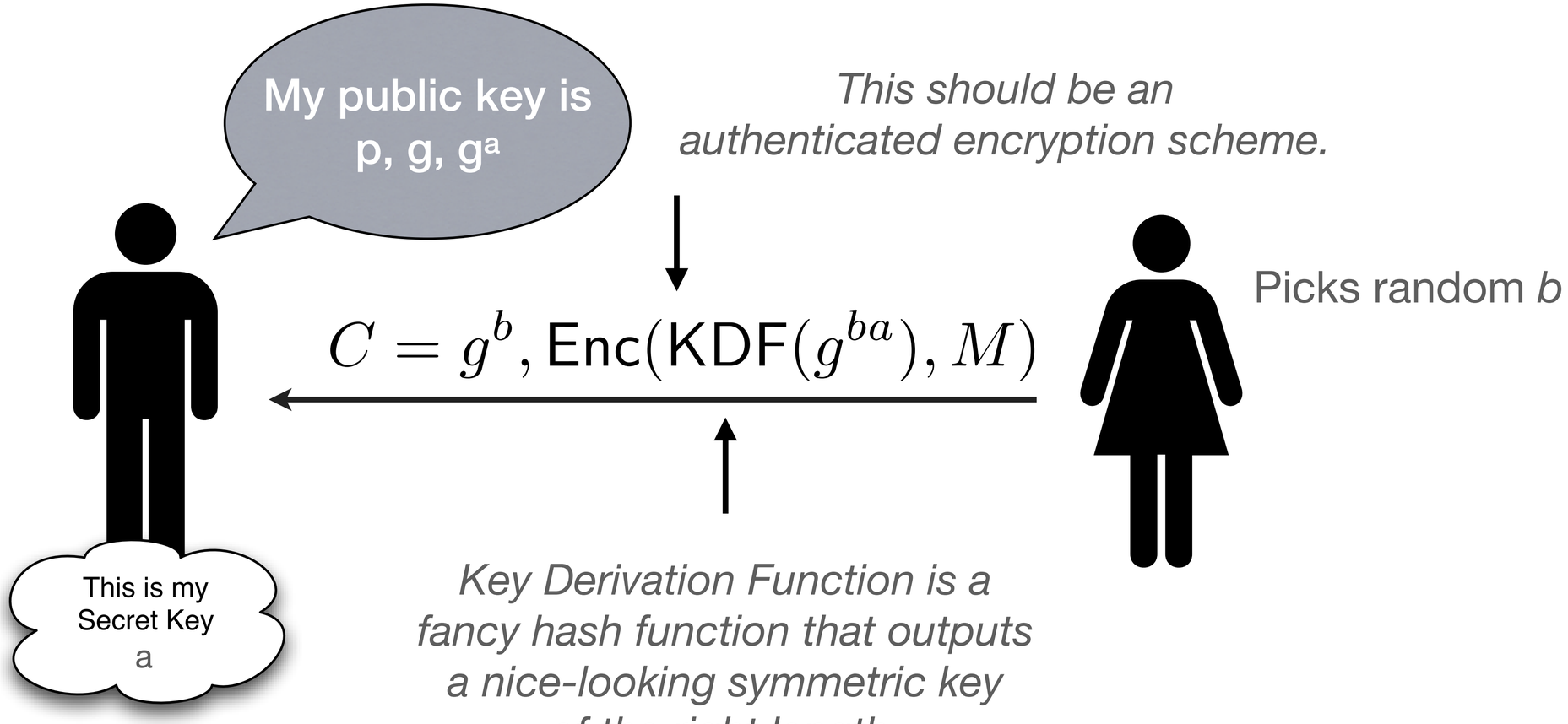
See Boneh-Shoup, Appendix A

How do we fix this?

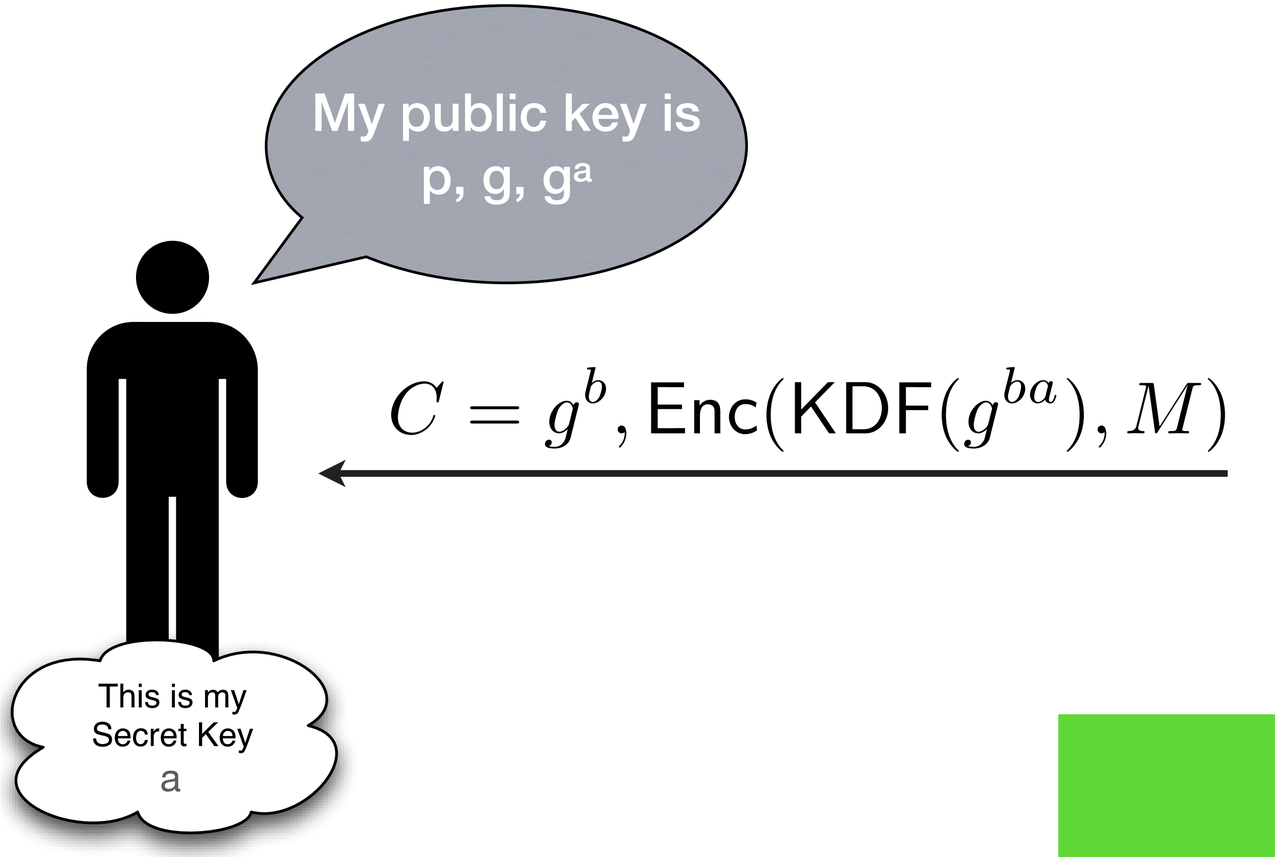
- Answer #1:
  - Always encode our message as an element of QR
  - (E.g., encode the message as *m,* compute M = m^2)
- Answer #2:
  - Use cyclic groups that don’t have subgroups (e.g., QRp!)
- Answer #3:
  - Don’t use multiplication to “encrypt” the group element

See Boneh-Shoup, Appendix A

How do we fix this?



How do we fix this?

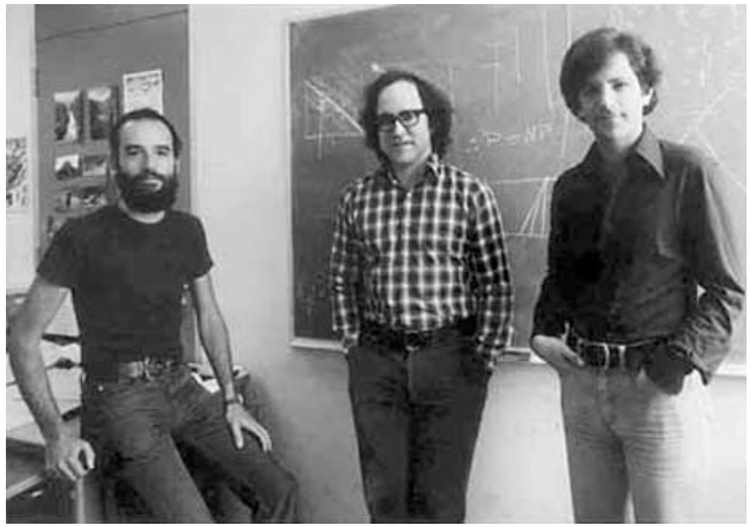


Examples:

DHIES scheme
ECIES scheme (elliptic curve)
Nacl's crypto_box (elliptic curve)

RSA

- Diffie-Hellman was the first key agreement scheme
- The use of D-H for public key encryption came later
- The first PKE was called RSA



Quick reminder: Euler/Fermat's little theorem

$$a^{\phi(N)} \equiv 1 \ mod \ N$$

$$\forall a, N : gcd(a, N) = 1$$

Reminder: $\phi(N)$ is the number of elements in {0, 1, …, N-1} that are relatively prime to N

Quick reminder: Euler/Fermat's little theorem

$$a^{\phi(N)} \equiv 1 \ mod \ N$$

$$\forall a, N : gcd(a, N) = 1$$

Implies….

$$a^{\phi(N)+1} \equiv 1 \cdot a \equiv a \ mod \ N$$

Quick reminder: Euler/Fermat's little theorem

$$a^{\phi(N)} \equiv 1 \ mod \ N$$

$$\forall a, N : gcd(a, N) = 1$$

Implies….

$$a^{\phi(N)+1} \equiv 1 \cdot a \equiv a \ mod \ N$$

Q: Can we split this into two separate keys (e, d)?

RSA Cryptosystem

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
  - Might be partially invertible

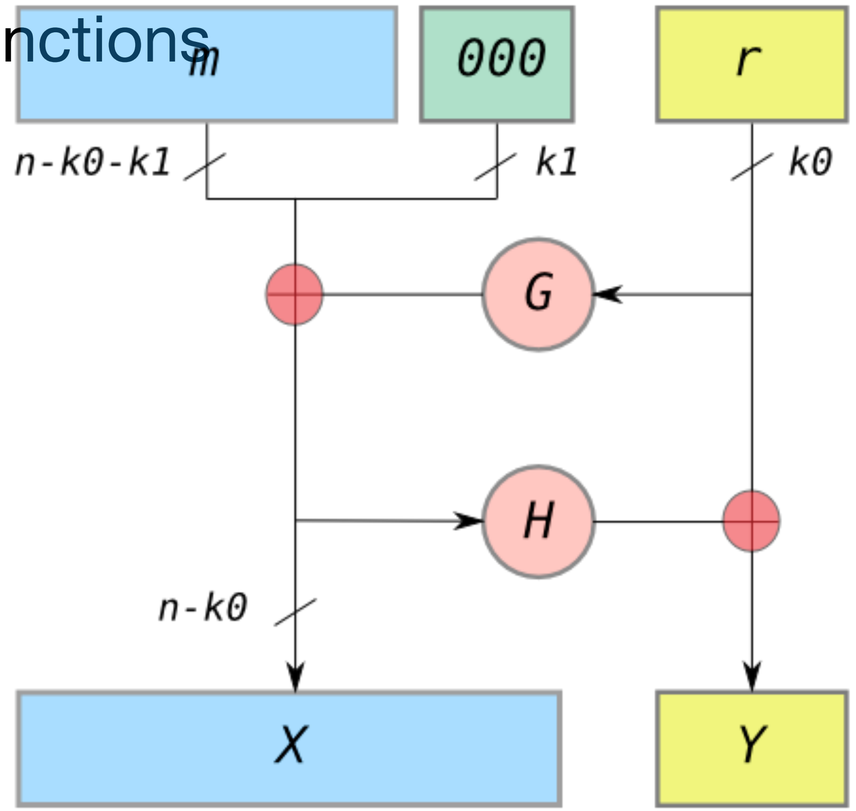
•Coppersmith’s attack: recover part of plaintext (when *m* and *e* are small)

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) Encryption	1,016
RSA (1024 bit key) Decryption	21,719

Hybrid Encryption

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

Key Strength

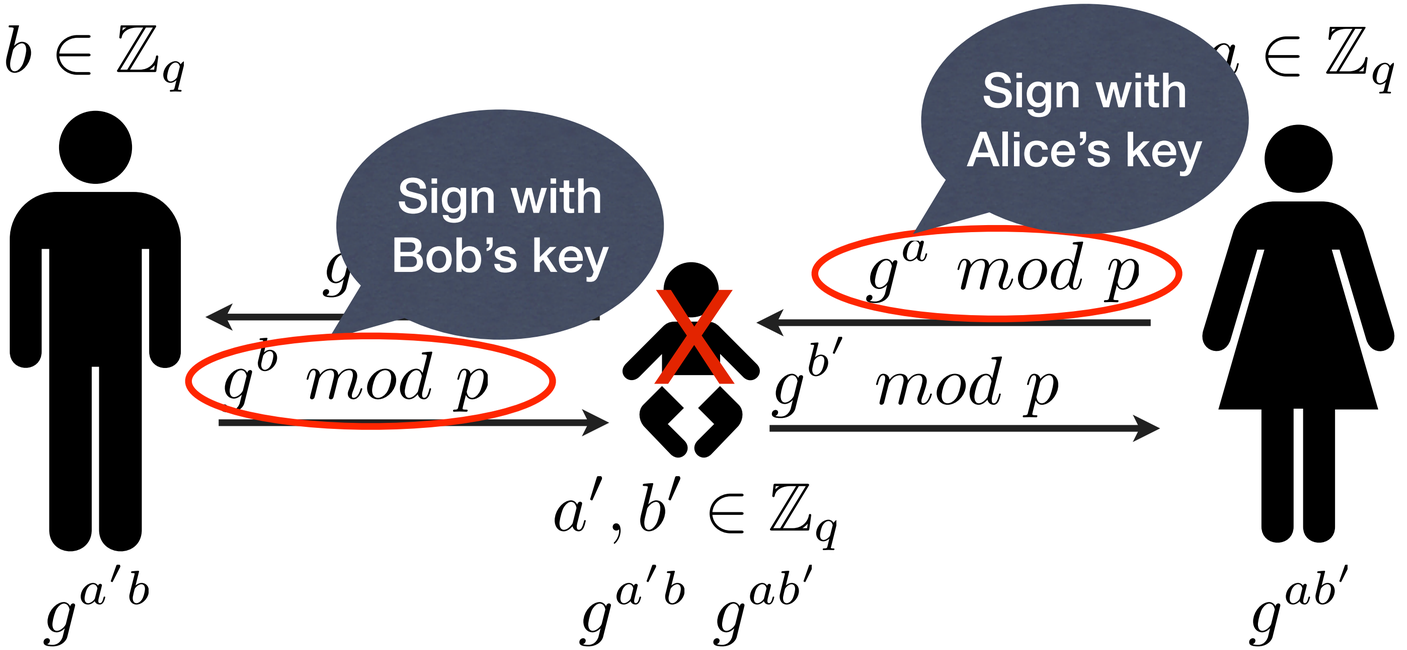
Level	Protection	Symmetric	Asymmetric	Discrete Logarithm Key	Discrete Logarithm Group	Elliptic Curve	Hash
1	Attacks in "real-time" by individuals *Only acceptable for authentication tag size*	32	-	-	-	-	-
2	Very short-term protection against small organizations *Should not be used for confidentiality 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

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:



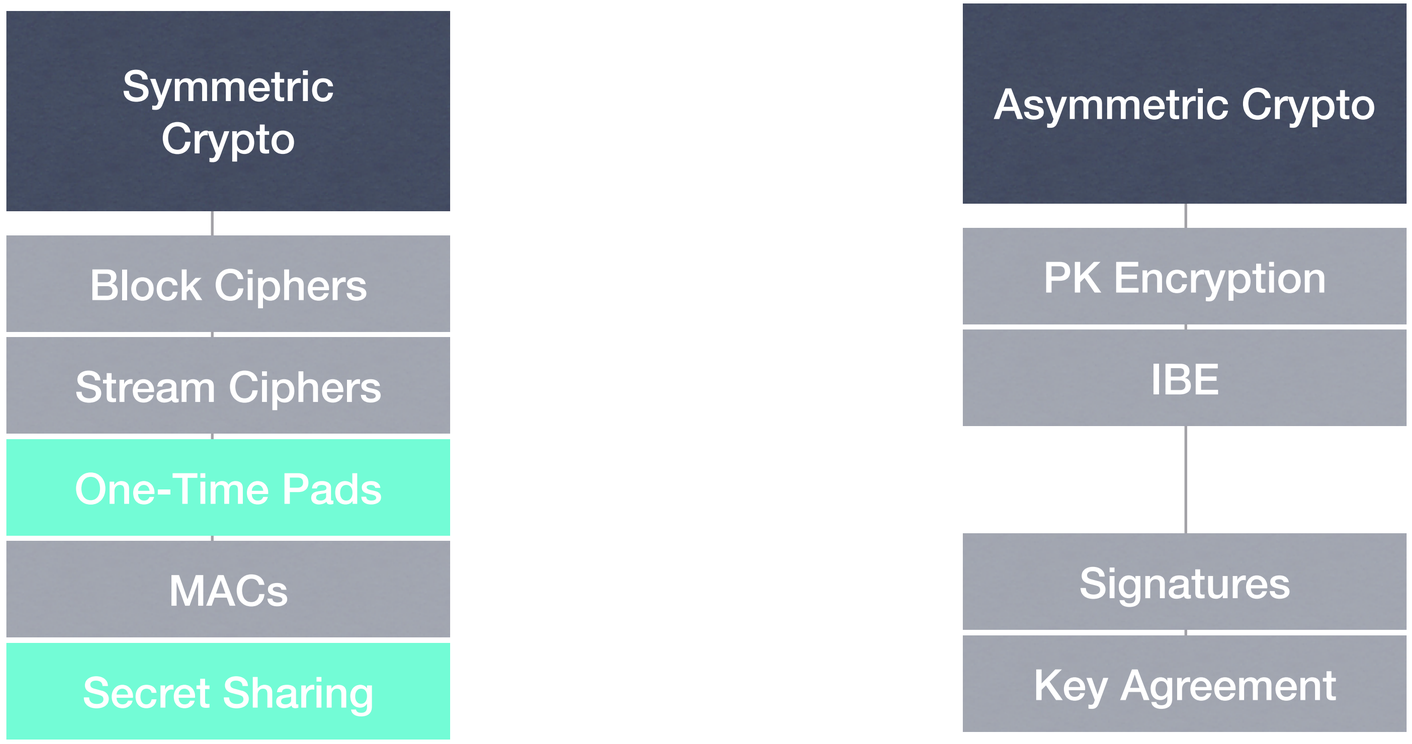
PKI & Certificates

- 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

Basic Primitives

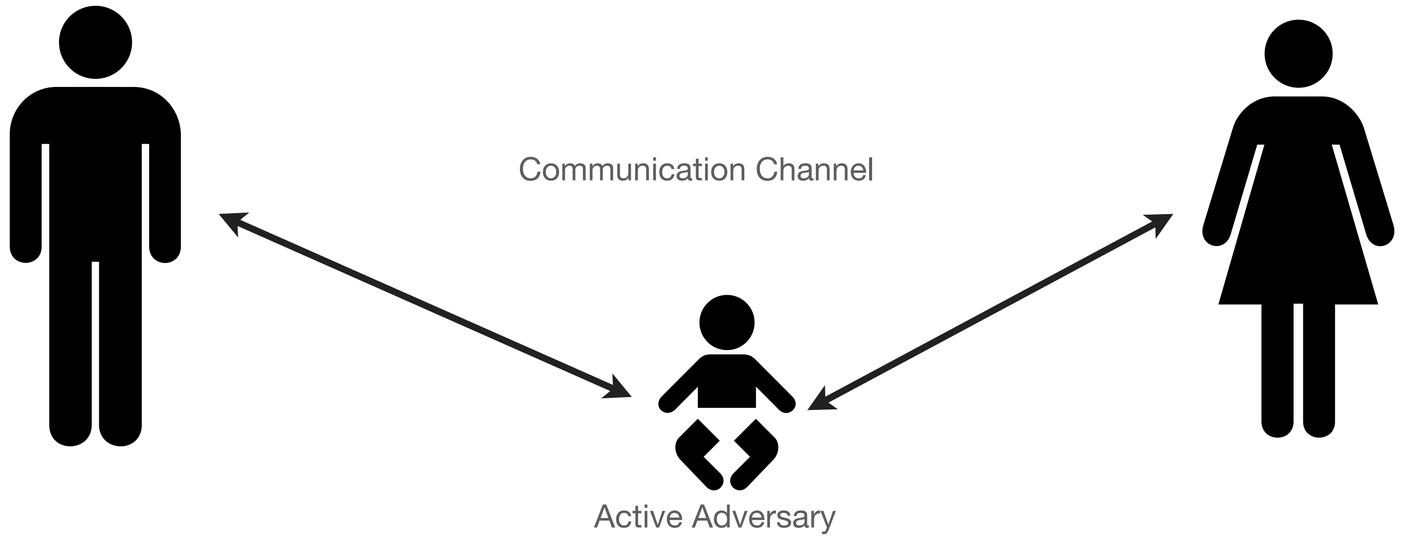


- Information Theoretic
- Complexity The

Next Time

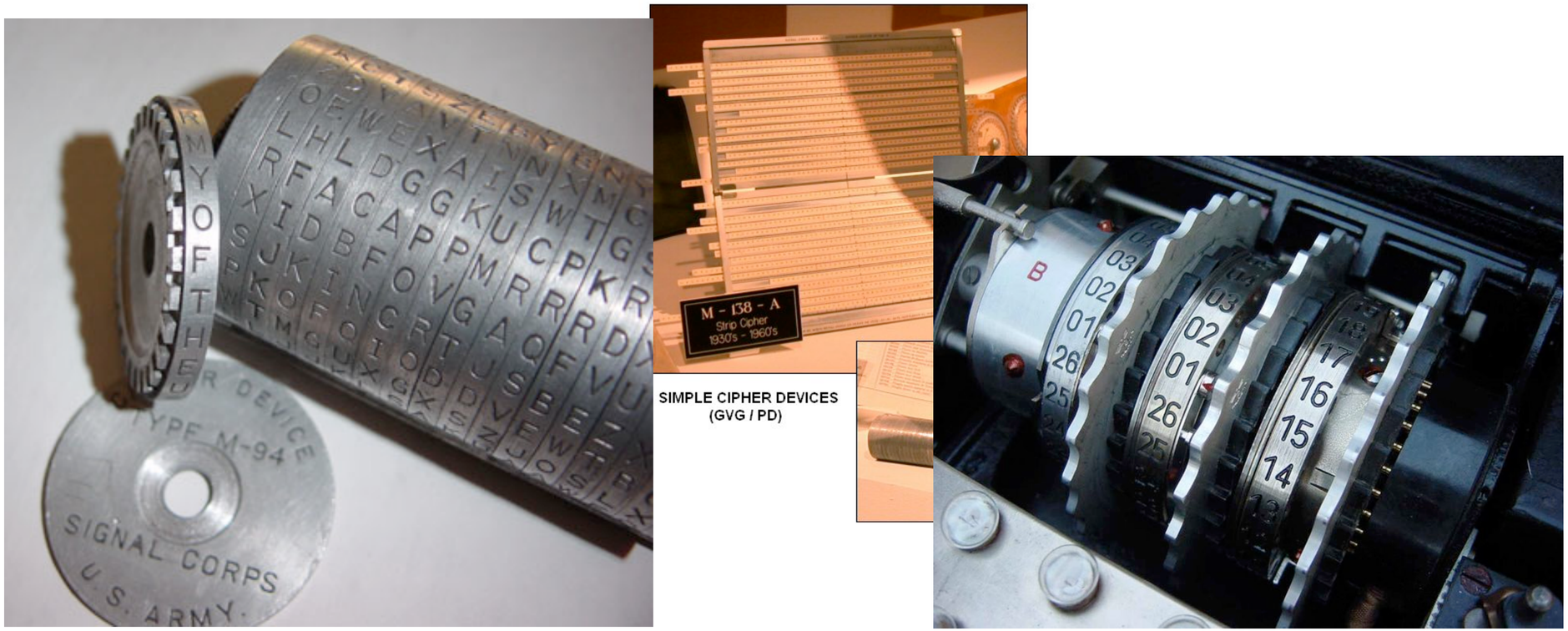
MACs

Authenticated Encryption



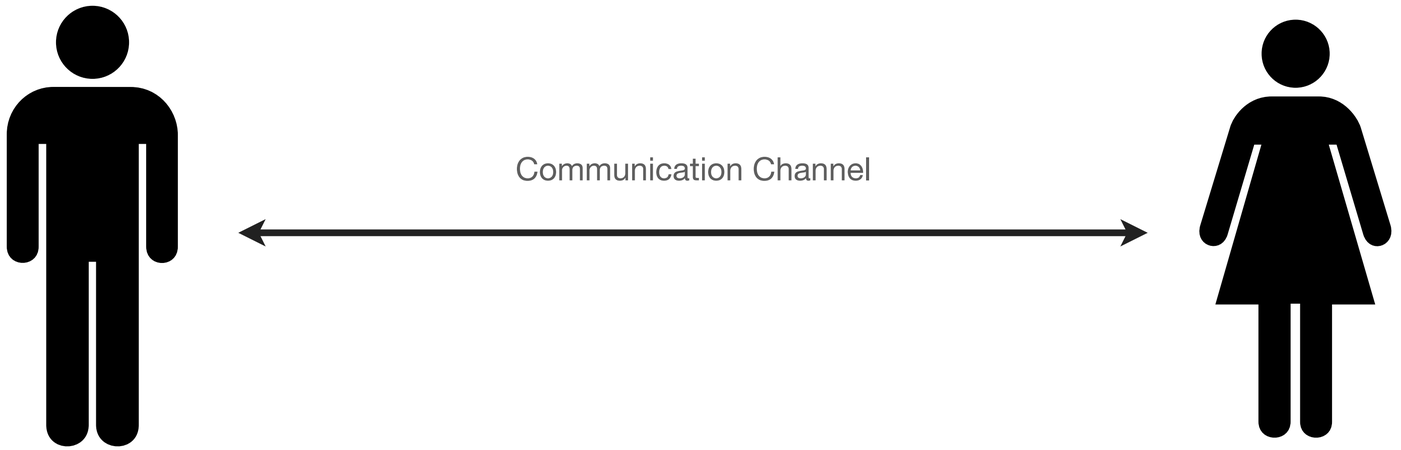
Convenience vs. Security

Mechanical Cryptography

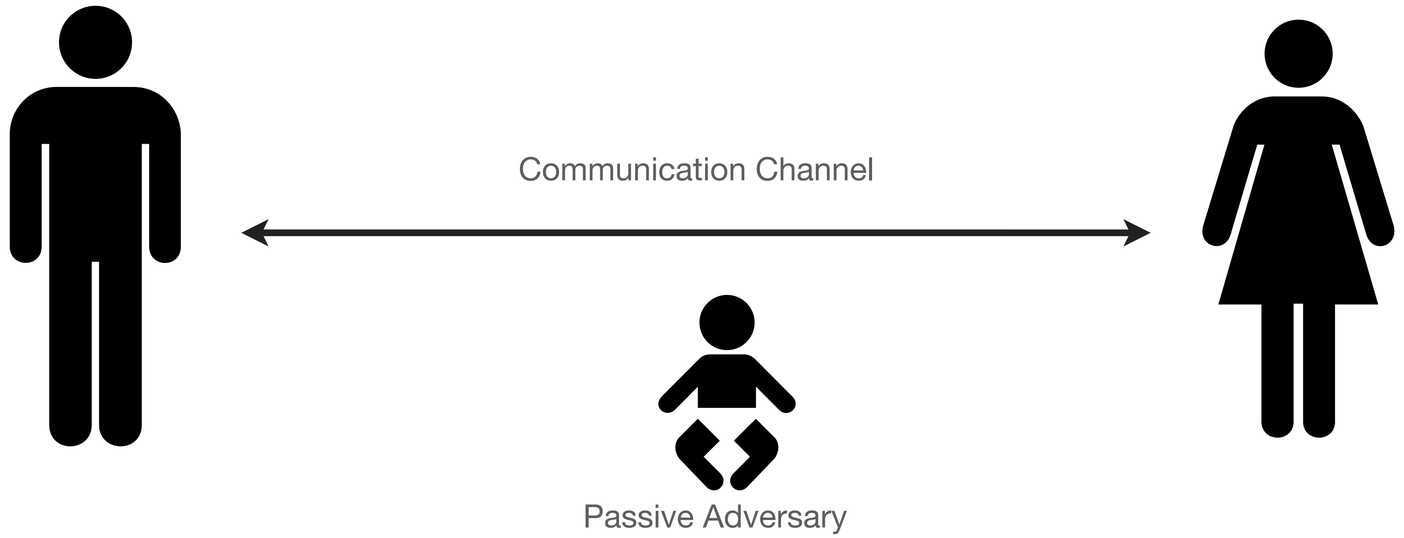


A quick note on ethics!

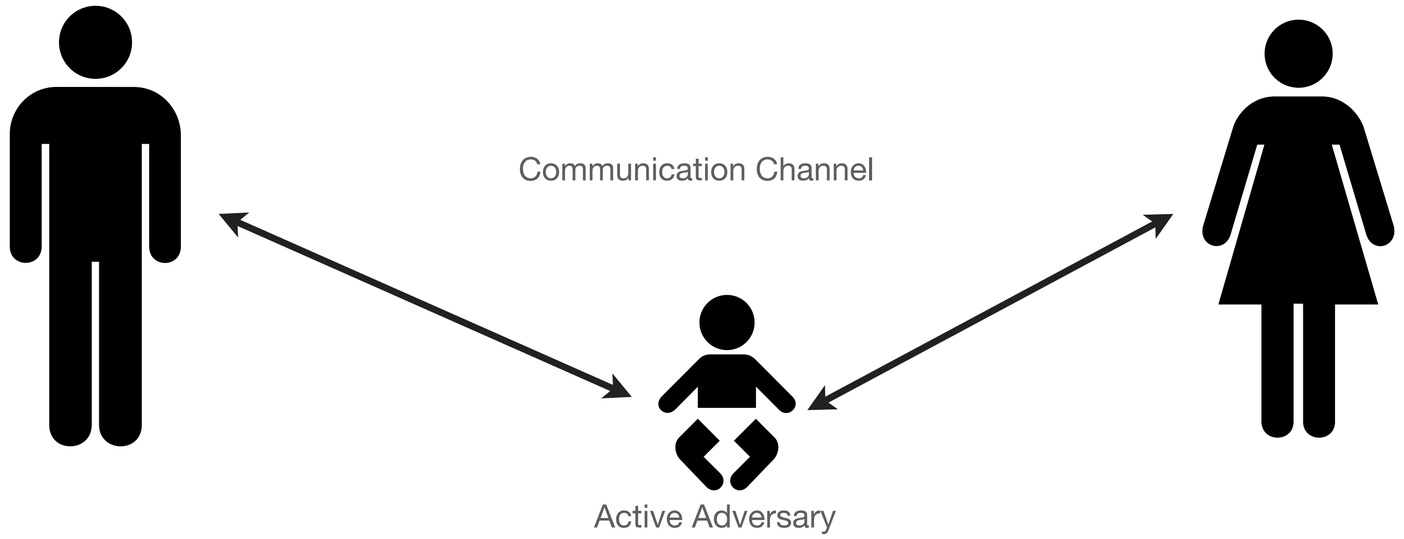
Communication Model



Communication Model



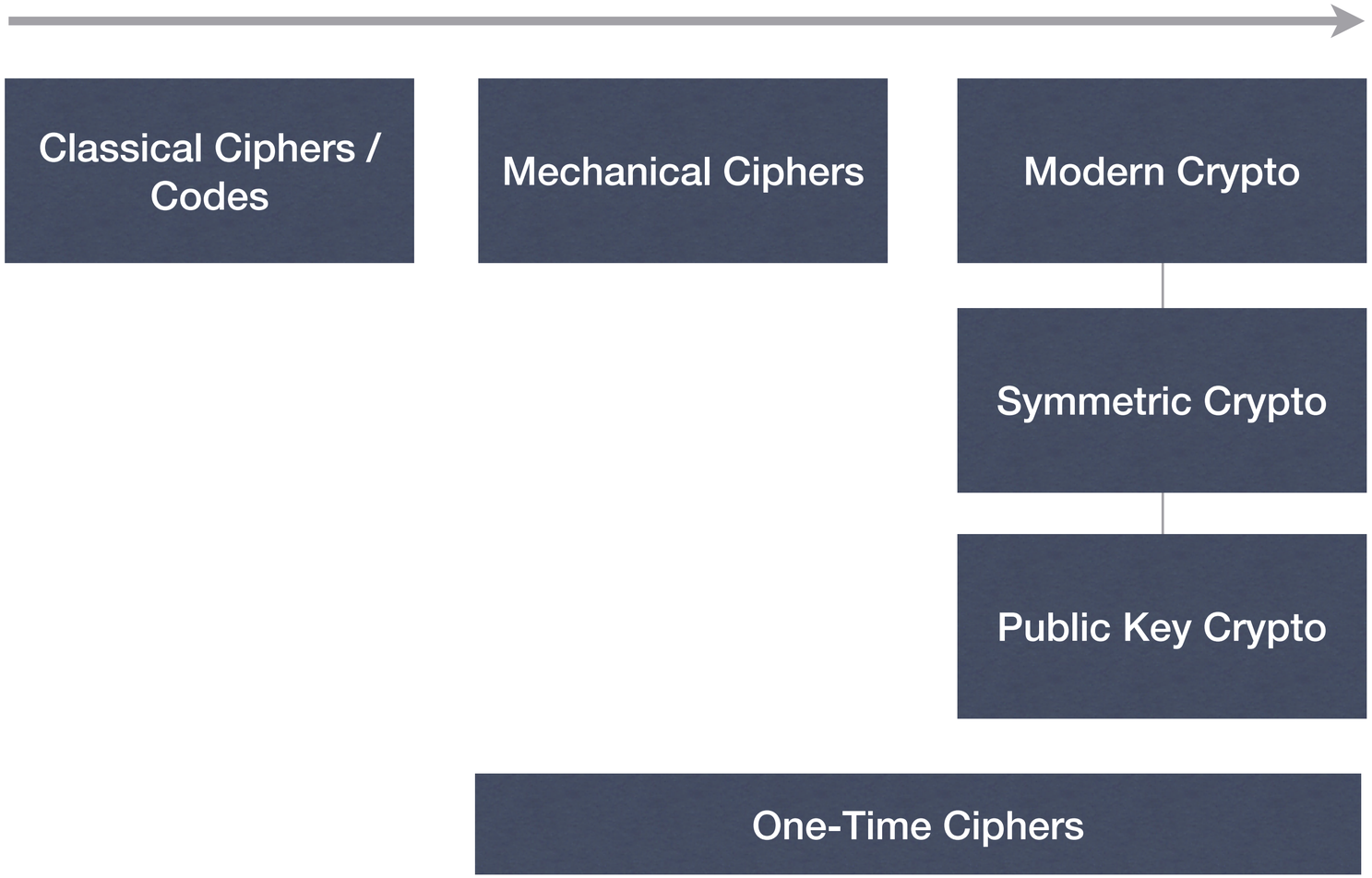
Communication Model



Secure Communication

- Two basic properties we like to achieve:
  - Data confidentiality
  - Data authenticity (“integrity”)
- Tools:
  - Encryption
  - Message Authentication Codes
  - Digital Signatures

History of Encryption



Classical Cryptography

- Beginning of time to 1900s or so
  - Shift (Caesar) cipher
  - Substitution ciphers
  - Polyalphabetic ciphers (Vigenère)
  - Digraph ciphers (Playfair)
  - A multitude of others...

<- Load New Puzzle

Tractability:11655

CRYPTOGRAM

Points 979

4/1/2009 0:21

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

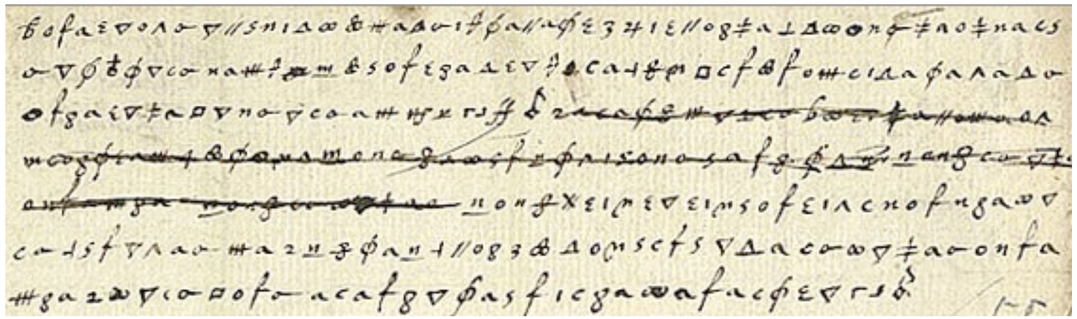
' P I G C G M N N U J C Y L I P G T Y T L P I Y T L M S F E P

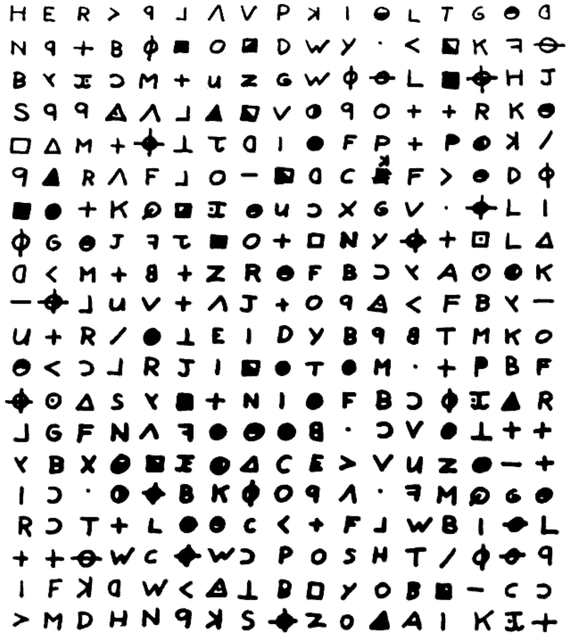
'

V Y K K N G M L G Y H P I M P U F E R T F O U F E ' N N L C F O

F E P F J Y P . ' - K F C Y H K M U

. ' -





A	G	R	P	T
B	I	K	C	Q
S	L	D	M	E
N	Y	W	F	X
G	J	H	O	Z

S	E	N	D	R	E	I	N	F	O	R	C	E	M	E	N	T	S
V	I	G	E	N	E	R	E	V	I	G	E	N	E	R	E	V	I
N	M	T	H	E	I	Z	R	A	W	X	G	R	Q	V	R	O	A

One-Time Ciphers

- 1900s
  - Vernam & Mauborgne's "Unbreakable" cipher

•Based on Baudot code for Teletypes

•Added (XORed) a random Key (sequence of bits) to a binary message

- Perfectly secure, provided:

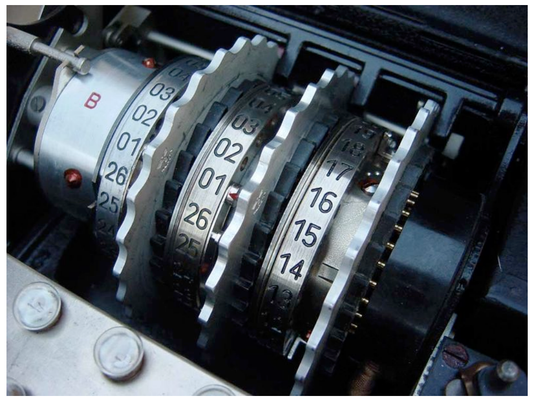
•key is perfectly random

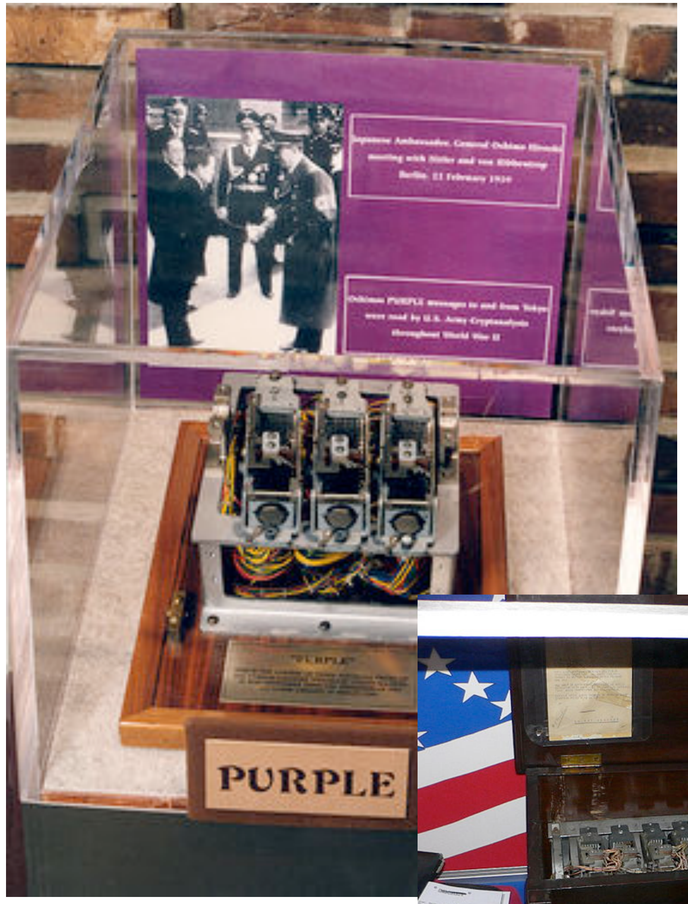
•key is at least as long as the message

•key is never re-used

Mechanical Cryptography

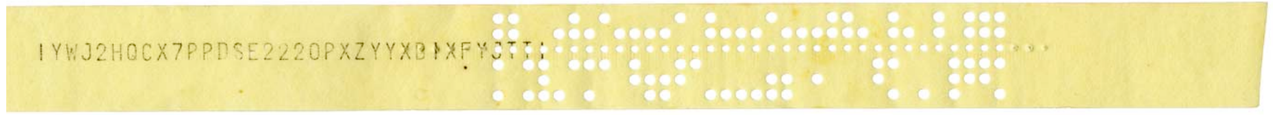
- 1900s
  - Mass production and usage of cipher devices
  - Rotor ciphers
  - Elec





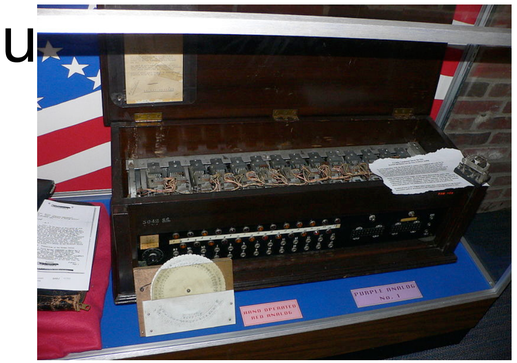
HAGELIN M-209 CIPHER MACHINE (GVG / PD)

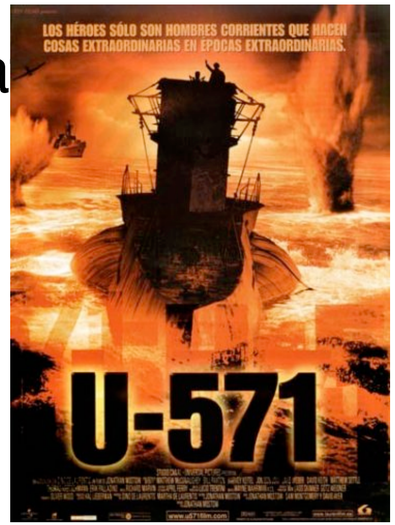

0015
AB CD EF GH I J KL MN OP QR ST UV WX YZ
AB CD EF GH I J KL MN OP QR ST UV WX YZ
0 AB
1 CD
2 EF
3 GH
4 I J
5 KL
6 MN
7 OP
8 ST
9 UV



Summary

- Most cryptosystems ultimately broken
  - Sophistication of the attackers outpaces that of the cryptosystem
  - Security relies on <u>secrecy of design</u>
  - Not evaluated for chosen plaintext, known plaintext a
  - Key generation/distribution procedu
  - It’s an arms race...





Kerckhoffs’ Principle(s)

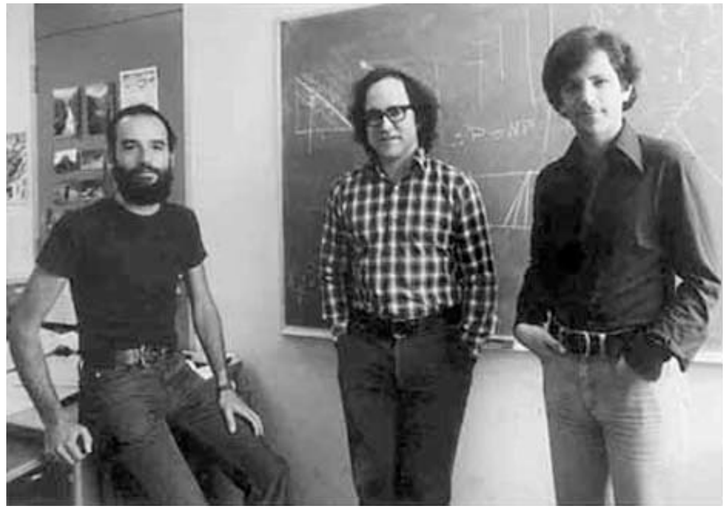
- Auguste Kerckhoffs (1835–1903)

Kerckhoffs' Principle(s)

2. It must not be required to be secret, and it must be able to fall into the hands of the enemy without inconvenience;

"The enemy knows the System"
-- Claude Shannon's Maxim

The 1970s



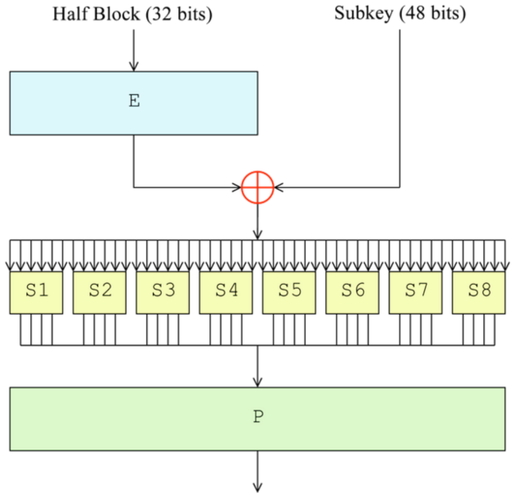
U.K. GCHQ

The Implications

- Exponential increase in study & usage of cryptography in industry, academia
- Wide-scale deployment of cryptographic systems
- Provable Security
  - Cryptographic Systems can be reduced to some hard mathematical problem

Data Encryption Standard

- Commercial-grade Block Cipher
  - 64-bit block size
  - 56 bit key (+ 8 bits parity)
  - “Feistel Network” Construction



Permutation

Permutation

Permutation Families

- Can’t have just one permutation
  - Alice & Bob know the permutation
    Adversary doesn’t
  - Permutation is “random” (ish)
  - But there are possible permutations
  - DES has a 56 bit key...

Block Cipher

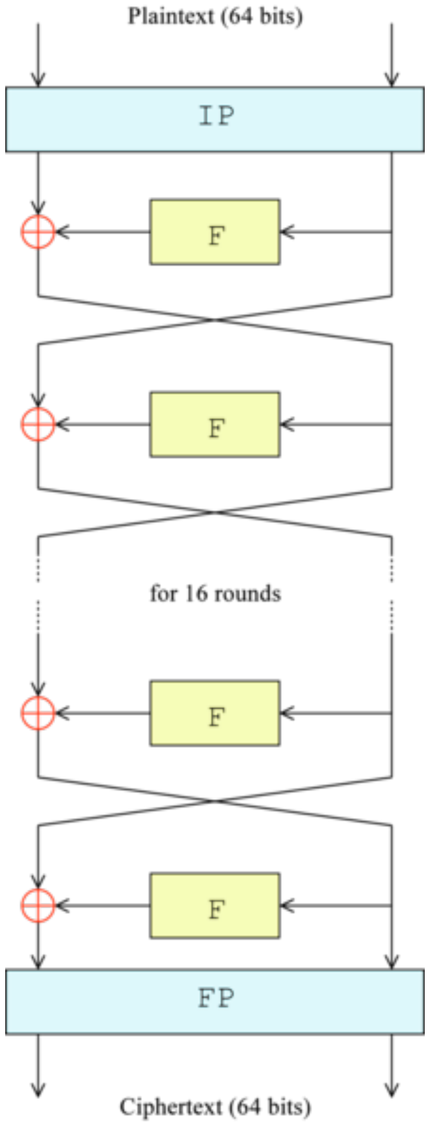
- Block cipher is a family of permutations
  - Indexed by a key (DES = 56 bit key)
  - “Pseudo-random”

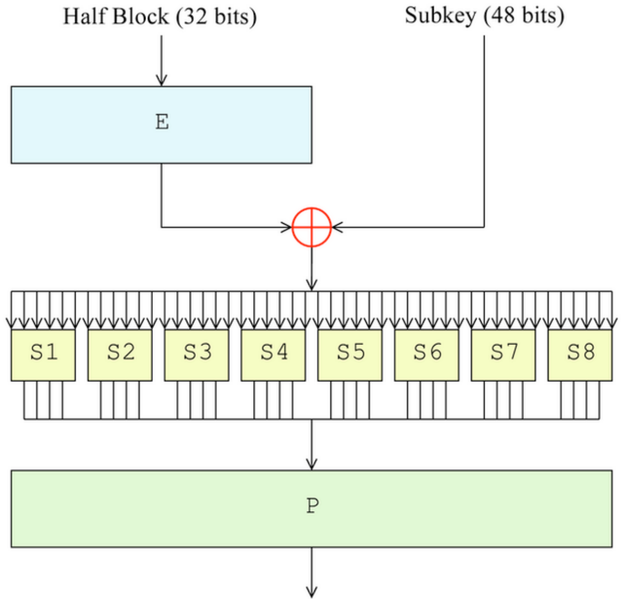
Block Cipher

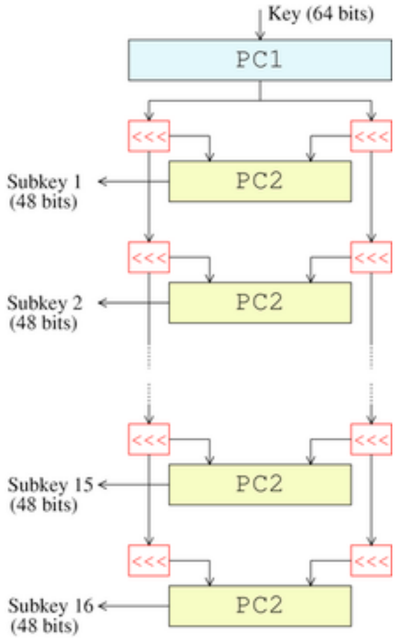
- Block cipher is a family of permutations
  - Indexed by a key (DES = 56 bit key)
  - Ideally: “Pseudo-random permutation (PRP)”

    (i.e., attacker who does not know the key can’t determine whether you’re using a random permutation, or a PRP)

DES: 64-bit Block, 56-bit Key

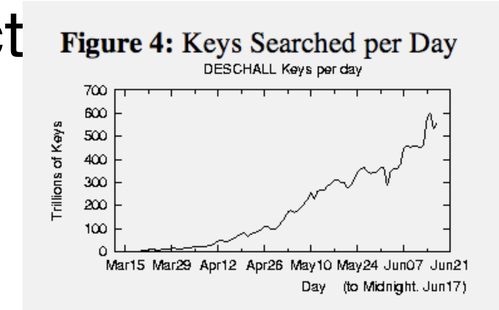


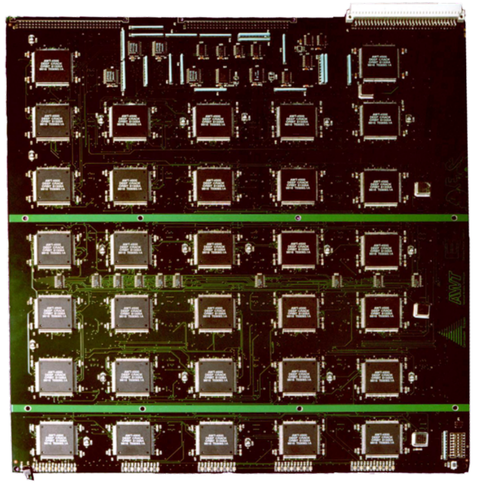




DES

- Some “clever” attacks on DES
  - However: practical weakness = 56 bit key size
  - Pract ES (now being deprecated)





U.S. Data-Scrambling Code Cracked With Homemade Equipment

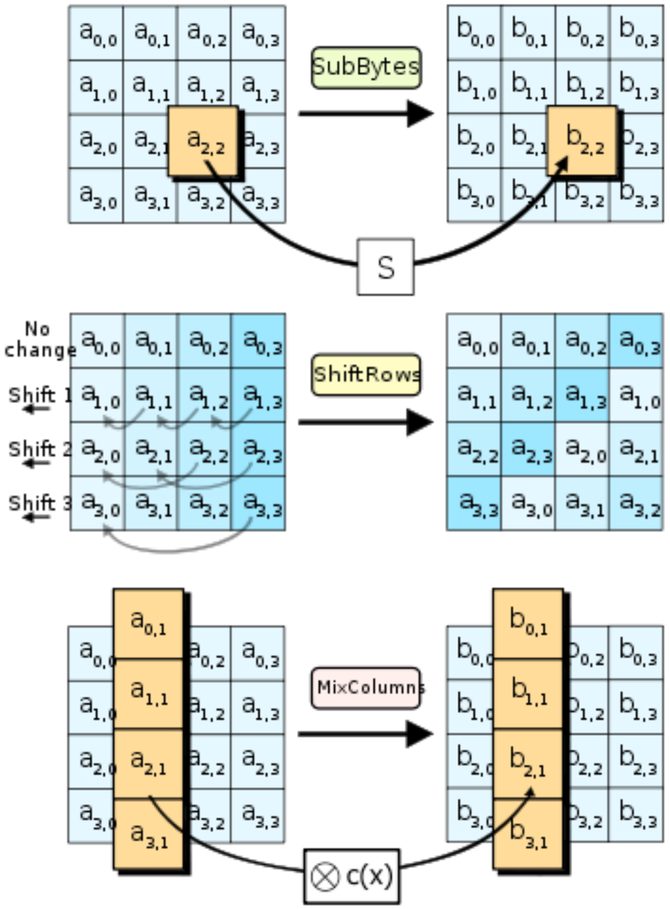
By JOHN MARKOFF

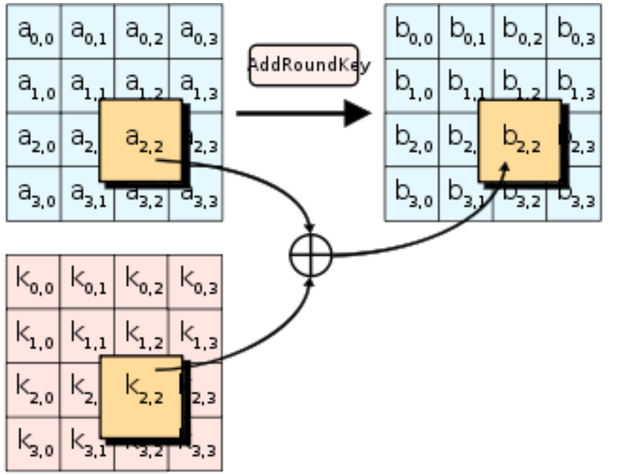
SAN FRANCISCO -- In a 1990s variant of a John Henry-style competition between man and machine, researchers using a homemade supercomputer have cracked the government's standard data-scrambling code in record time -- and have done it by out-calculating a team that had harnessed thousands of computers, including some of the world's most powerful.

AES

- NIST open competition:
  - Fast in software & hardware
  - Larger block size (128 bit)
  - Longer keys (128/192/256-bit)
- 5 finalists:
  - MARS, RC6, Rijndael, Serpent, and Twofish

AES: 128-bit Block, 128/192/256-bit Key



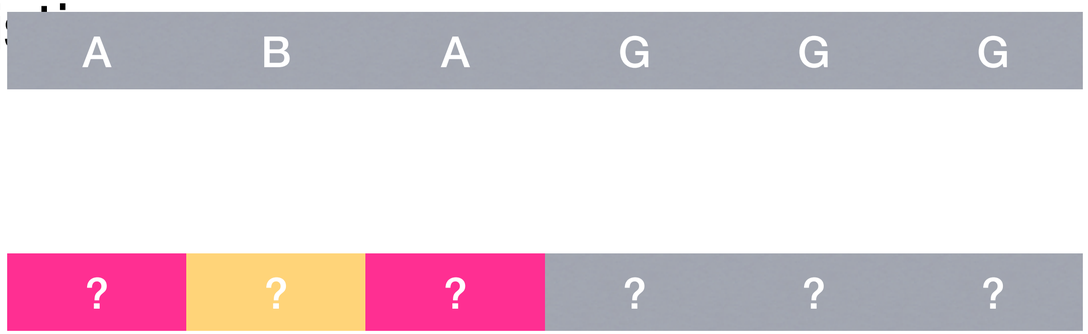


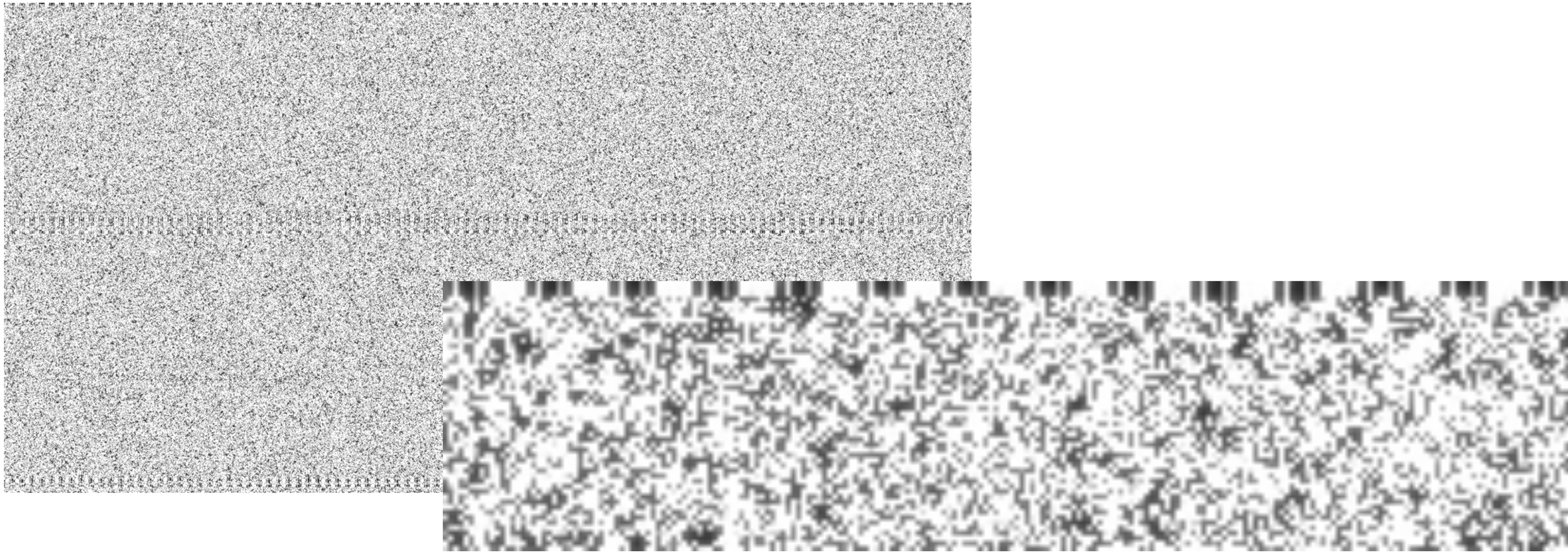
Attacks on AES

- Attacks on the design:
  - All theoretical
  - Work on reduced-round versions
  - Some debate about whether estimates are correct
- Side channel attacks:
  - Timing, cache hits & timing

Using Block Ciphers

- ECB Mode: Encrypt each block separately
  - Bad idea!
  - May reveal distribution of the plaintext
  - Totally determini





Defining Security

- What we'd like from our encryption scheme?
  - Ciphertext doesn't leak *any* info about plaintext
  - Even if Adversary knows a lot about the plaintext distribution
  - Even if Adversary can choose the plaintext distribution

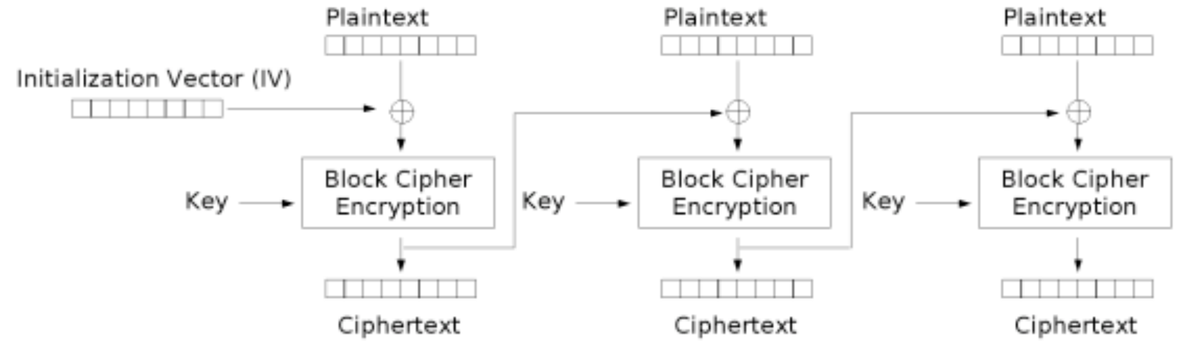
Defining Security

- Semantic Security
  - “Indist. under chosen plaintext attack”
    (IND-CPA)
  - Adversary w/ the ciphertext learns as much as Adversary w/o the ciphertext

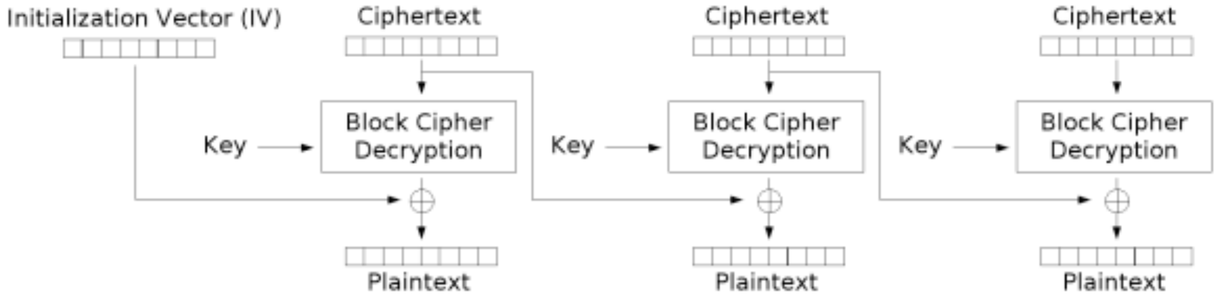
Using Block Ciphers

- ECB is not semantically secure, hence we use a “mode of operation”
  - e.g., CBC, CTR, CFB, OFB (and others)
- These provide:
  - Security for multi-block messages
  - Randomization (through an Initialization Vector)

CBC Mode



Cipher Block Chaining (CBC) mode encryption



Cipher Block Chaining (CBC) mode decryption

Security of CBC

- Is CBC secure?
  - Yes, assuming a secure block cipher
  - IND-CPA
- Easy to use wrong...
  - Most imporant: use a unique & random IV!

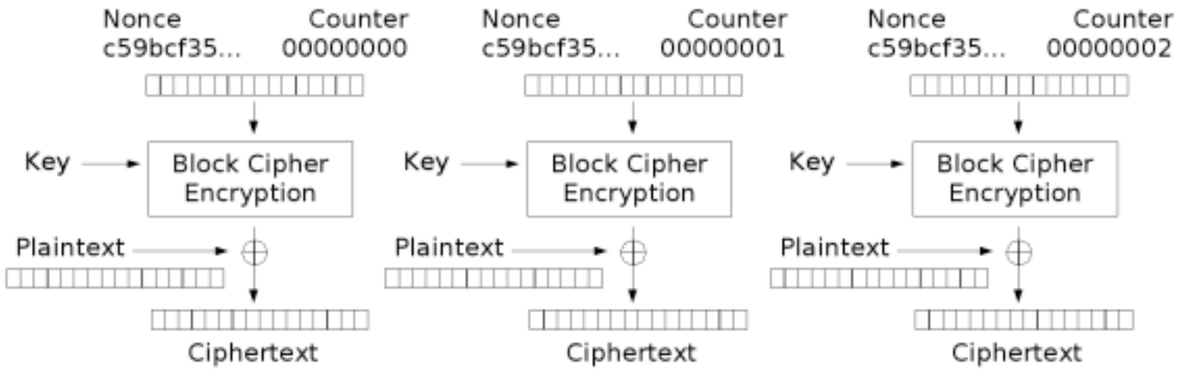
The size of the frame of data to be encrypted or decrypted (i.e. how often a new CBC chain is started) depends on the particular application, and is defined for each in the corresponding format specific books of this specification. Unless otherwise specified, the Initialization Vector used at the beginning of a CBC encryption or decryption chain is a constant, $iv_{0,}$ which is:

$0BA0F8DDFEA61FB3D8DF9F566A050F78_{16}$

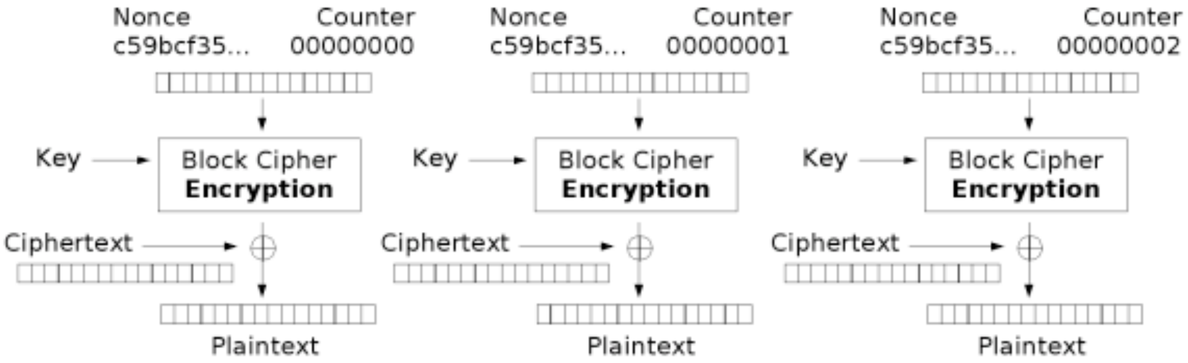
Advanced Access Content System (AACS)

Introduction and Common Cryptographic Elements

CTR Mode



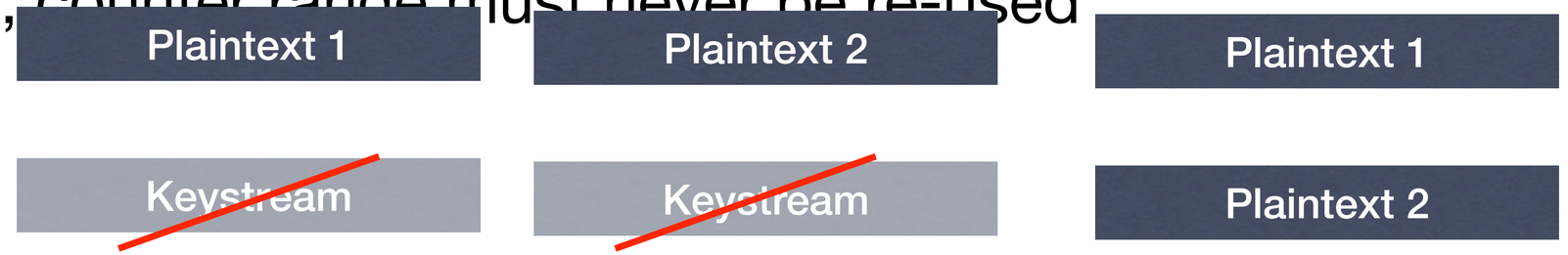
Counter (CTR) mode encryption



Counter (CTR) mode decryption

Security of CTR

- Yes, assuming secure block cipher
- However, counter range must never be re-used



- Similar example: MS Word 2003
  - (they used RC4, but same problem)

Point of order

- Proofs of security:
  - We don’t know how to prove that DES or AES are secure block ciphers
  - But if we assume that the block ciphers are secure:

•We can prove that CBC & CTR
are secure encryption modes.

Malleability

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

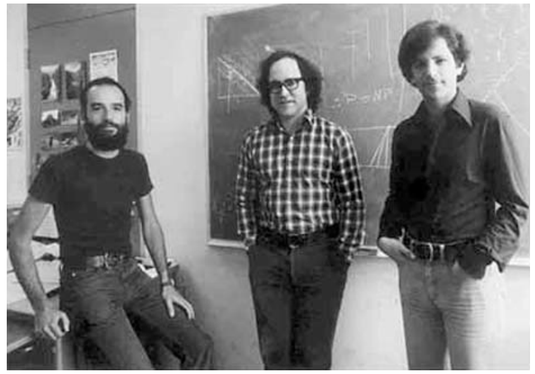
- Definitions of Security
  - Existential Unforgeability under CMA
- Examples:
  - HMAC (based on hash functions)
  - CMAC (block ciphers)

Presentations

- Lest I forget... (2/19 or 2/26)
- My suggestions:
  - Random Number Generation
  - Attacks on WinZip
  - Cracking Passwords (Rainbow Tables)
  - But... other ideas welcome!

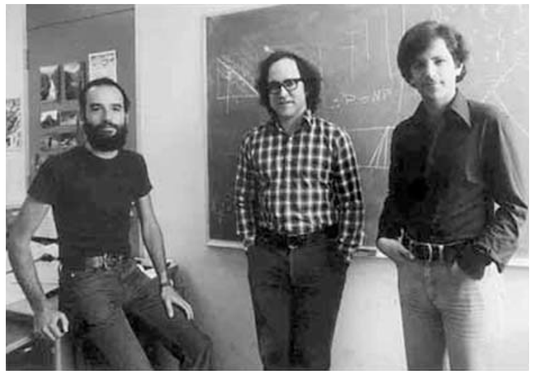
Next Time

- On through the 70s!
  - Key agreement
  - Public Key Encryption



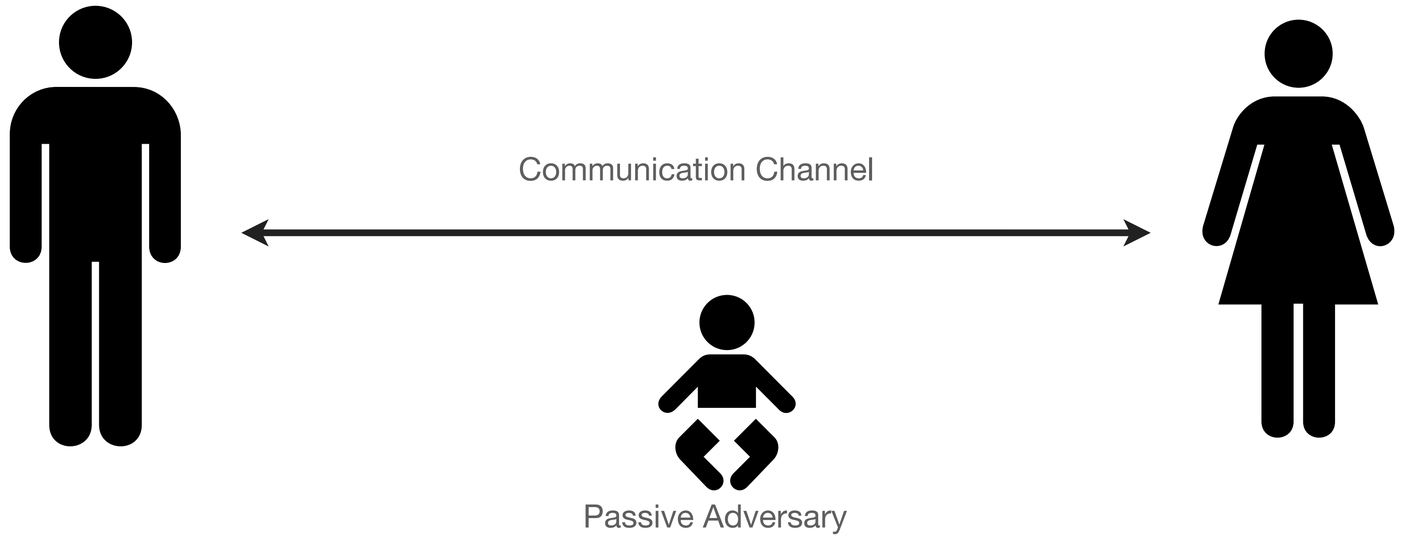
Asymmetric Crypto

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

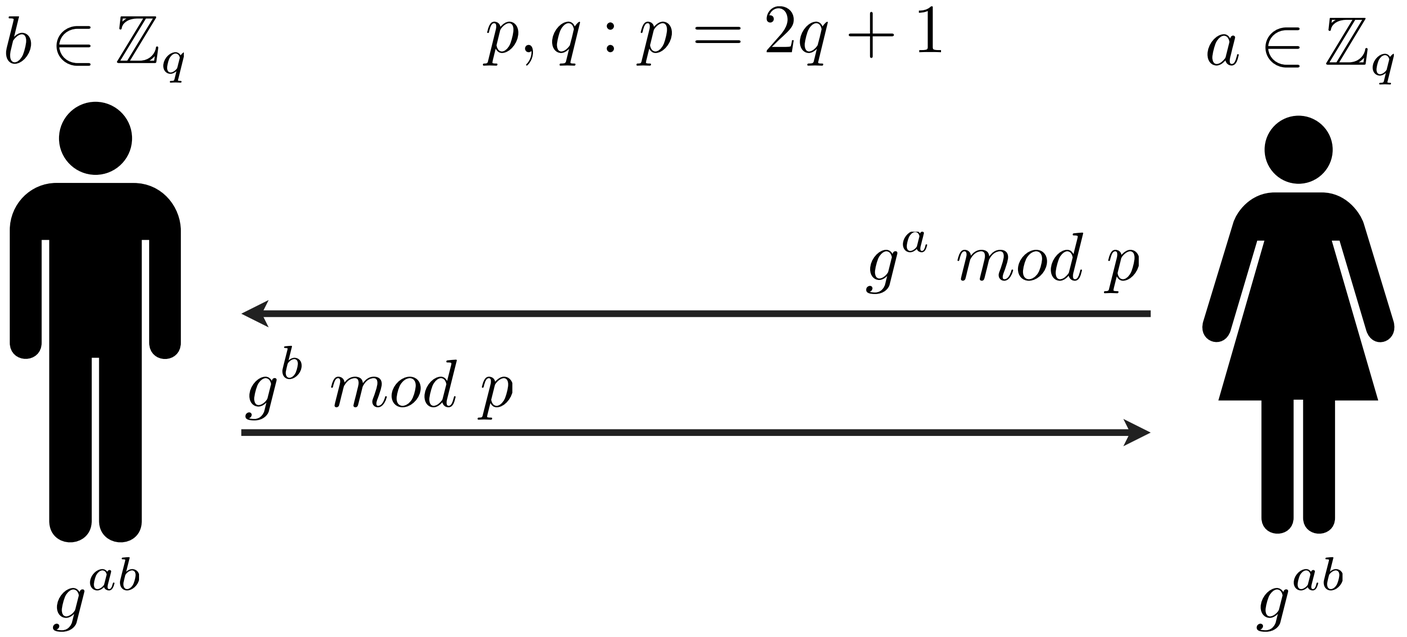


Key Agreement

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

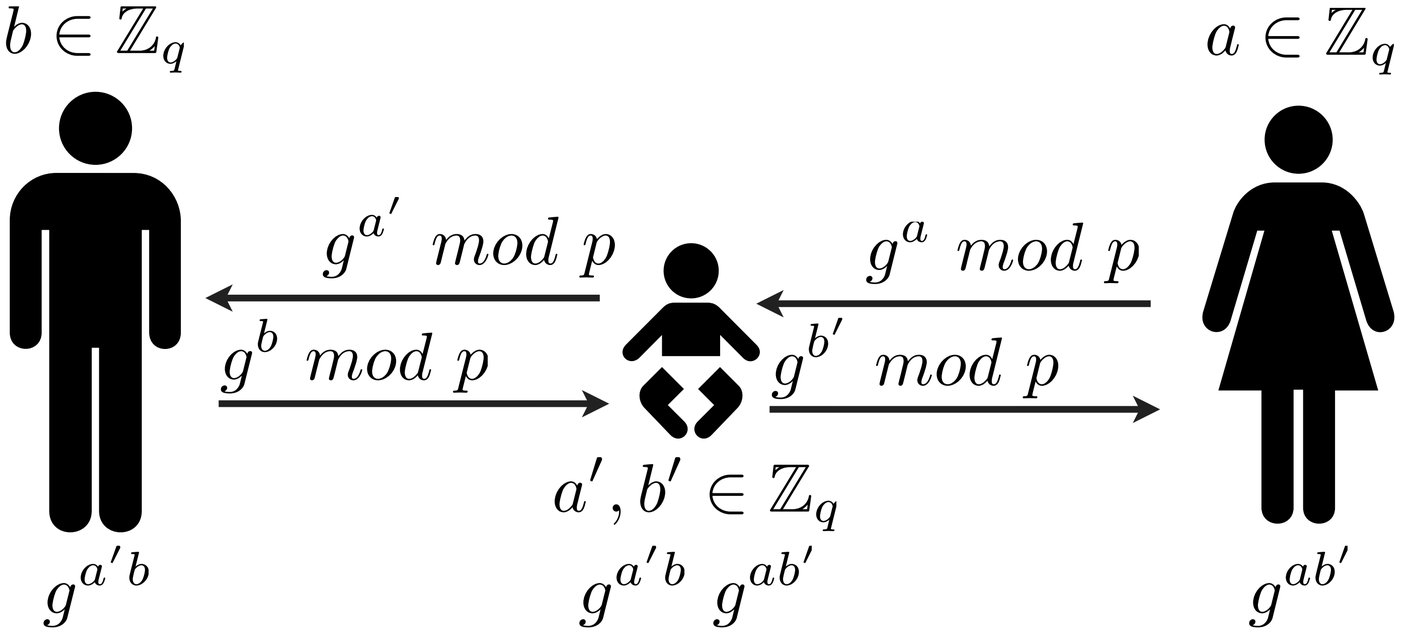


D-H Protocol



Man in the Middle

- Assume an active adversary:



Man in the Middle

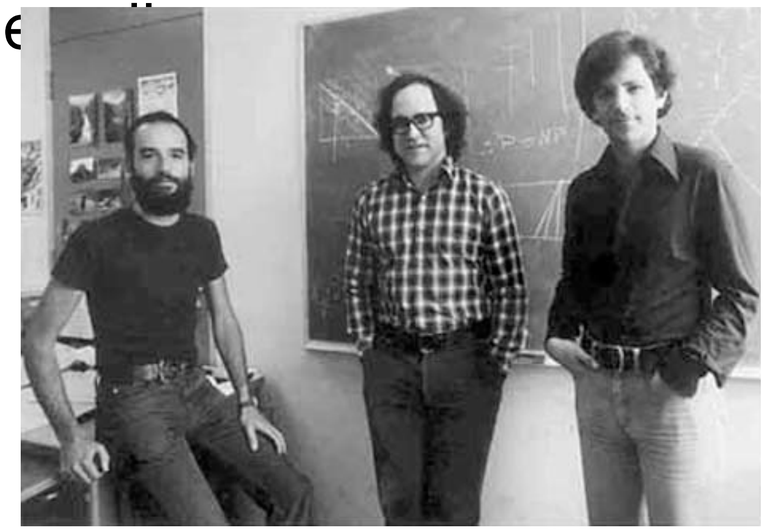
- Caused by lack of authentication
  - D-H lets us establish a shared key with anyone... but that's the problem...
- Solution: Authenticate the remote party

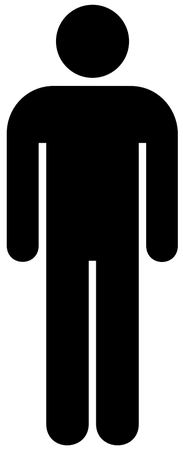
Preventing MITM

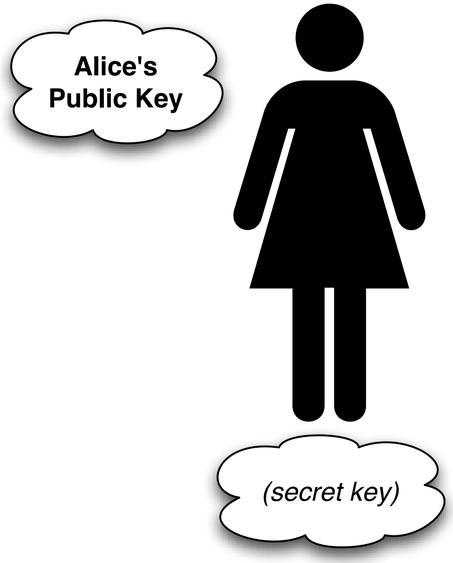
- Verify key via separate channel
- Password-based authentication
- Authentication via PKI

Public Key Encryption

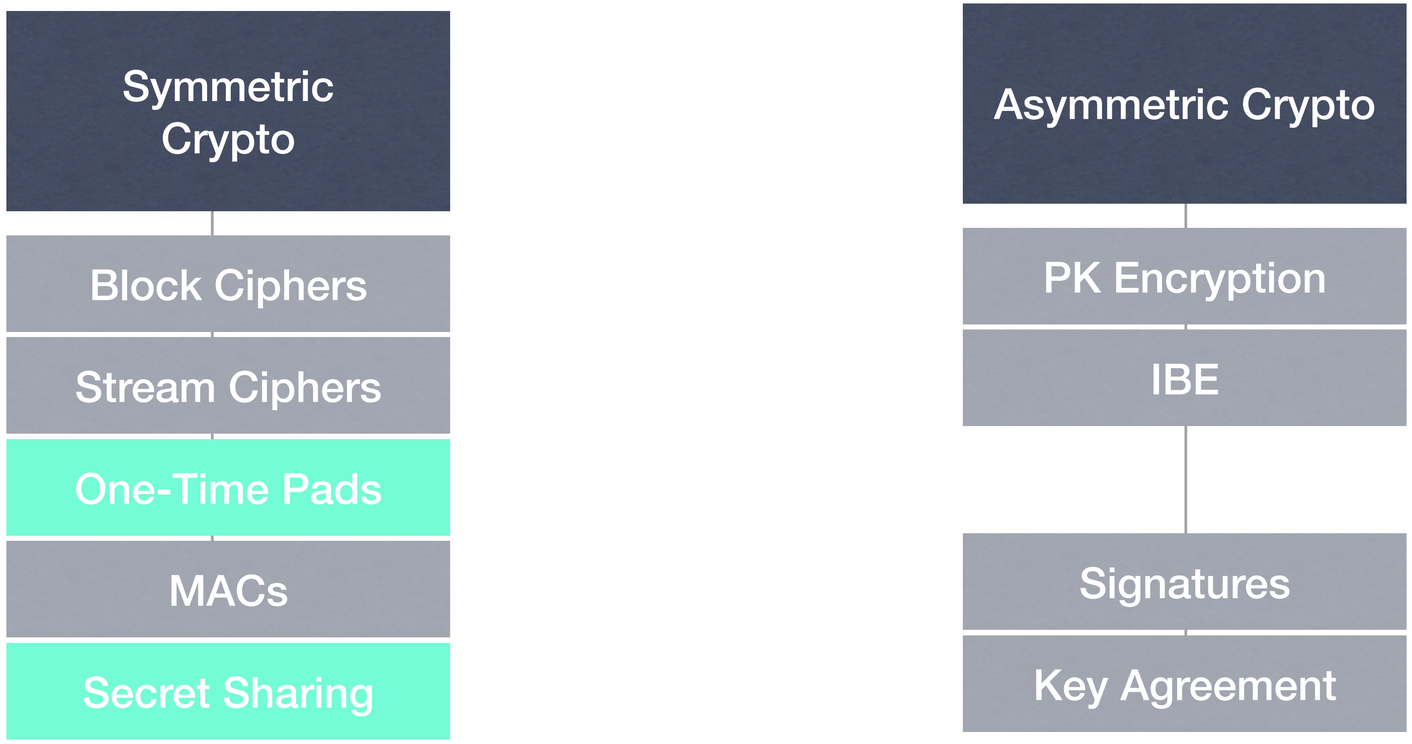
- What if our recipient is offline?
  - Key agreement protocols are interactive
  - e.g., want to send an e






Alice's
Public Key
(secret key)

Basic Primitives

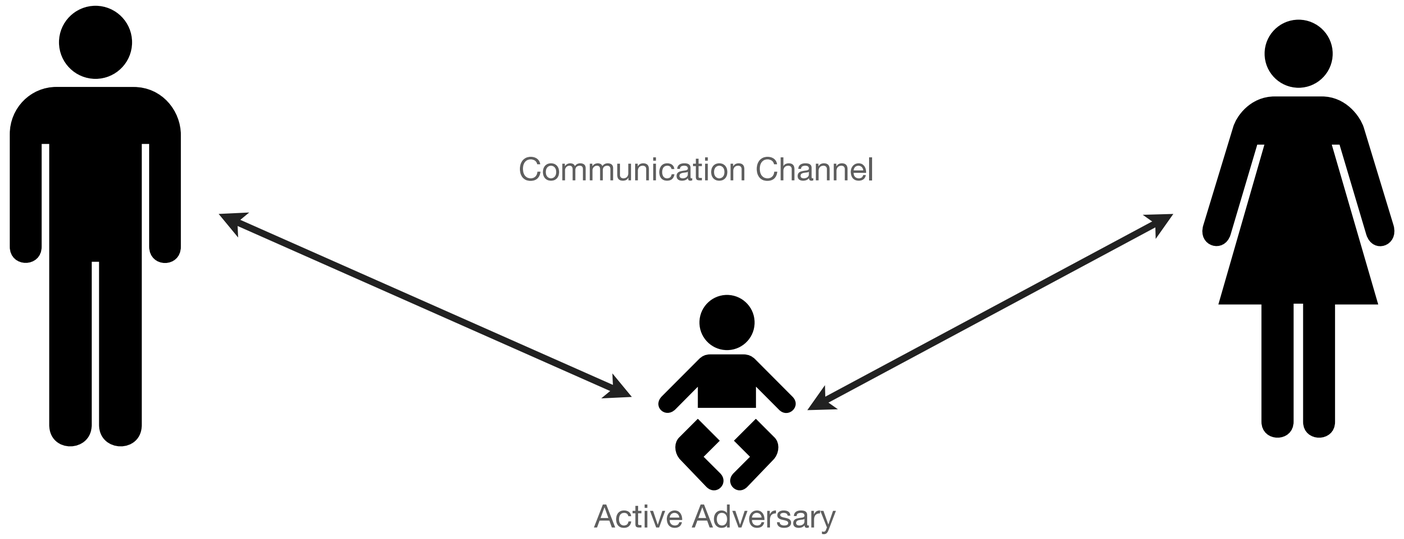


- Information Theoretic
- Complexity The

Next Time

MACs

Authenticated Encryption



Convenience vs. Security

Mechanical Cryptography