Introduction to Cryptography

Susan Hohenberger

JOHNS HOPKINS
UNIVERSITY

Cryptography

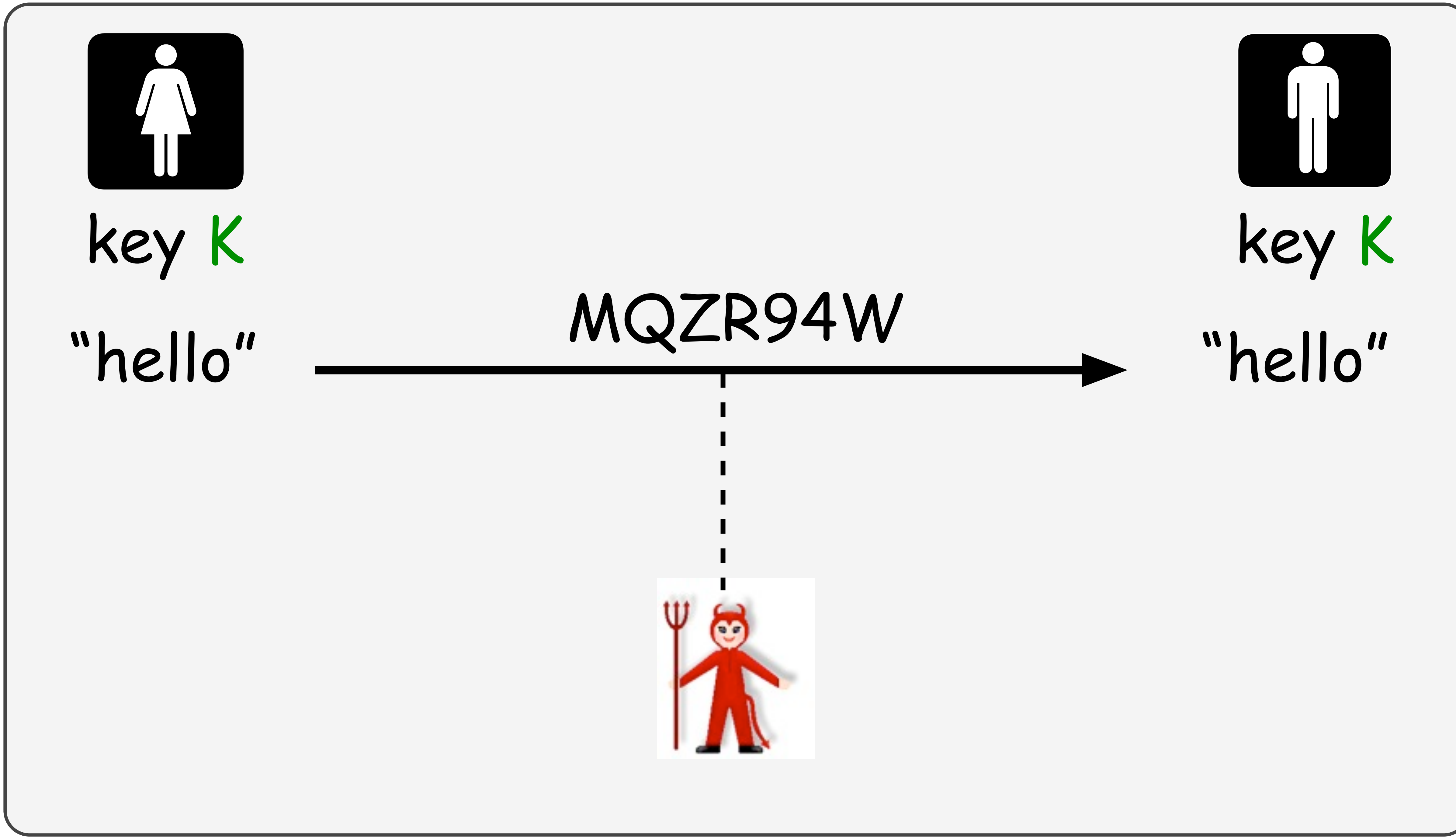
-- from art to science

-- more than just encryption

-- essential today for non-military applications

Symmetric Crypto

Shared secret K => Eve can't eavesdrop



Classic Ciphers

The Shift Cipher

A = 0, B = 1, C = 2, ..., Z = 25

$$x, y, K \in Z_{26}$$

$$e_K(x) = x + K \bmod 26$$

$$d_K(y) = y - K \bmod 26$$

The Shift Cipher

$A = 0,\ B = 1,\ C = 2,\ \ldots,\ Z = 25$

$$x, y, K \in Z_{26}$$
$$e_K(x) = x + K \bmod 26$$
$$d_K(y) = y - K \bmod 26$$

Cryptanalysis? Try 13 times on average.

Example $(K = 11)$:

W	E	W	I	L	L	M	E	E	T	A	T	M	I	D	N	I	G	H	T
22	4	22	8	11	11	12	4	4	19	0	19	12	8	3	13	8	6	7	19
⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓
7	15	7	19	22	22	23	15	15	4	11	4	23	19	14	24	19	17	18	4
H	P	H	T	W	W	X	P	P	E	L	E	X	T	O	Y	T	R	S	E

Example from D.R. Stinson (CRC Press)

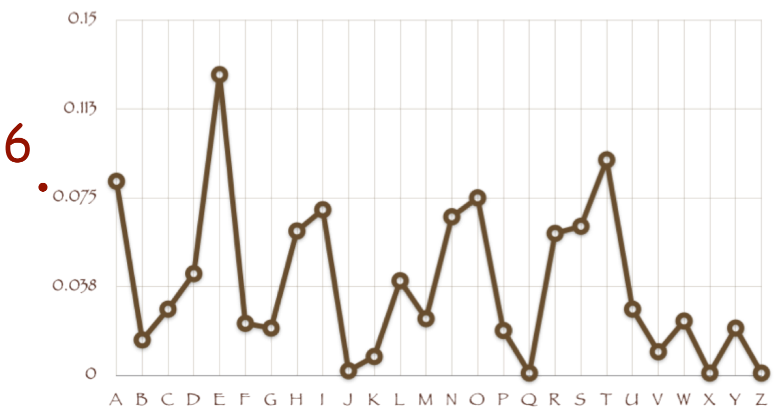
The Substitution Cipher

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

W	E	W	I	L	L	M	E	E	T	A	T	M	I	D	N	I	G	H	T
⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓	⇓
K	H	K	Z	B	B	T	H	H	M	X	M	T	Z	A	S	Z	O	G	M

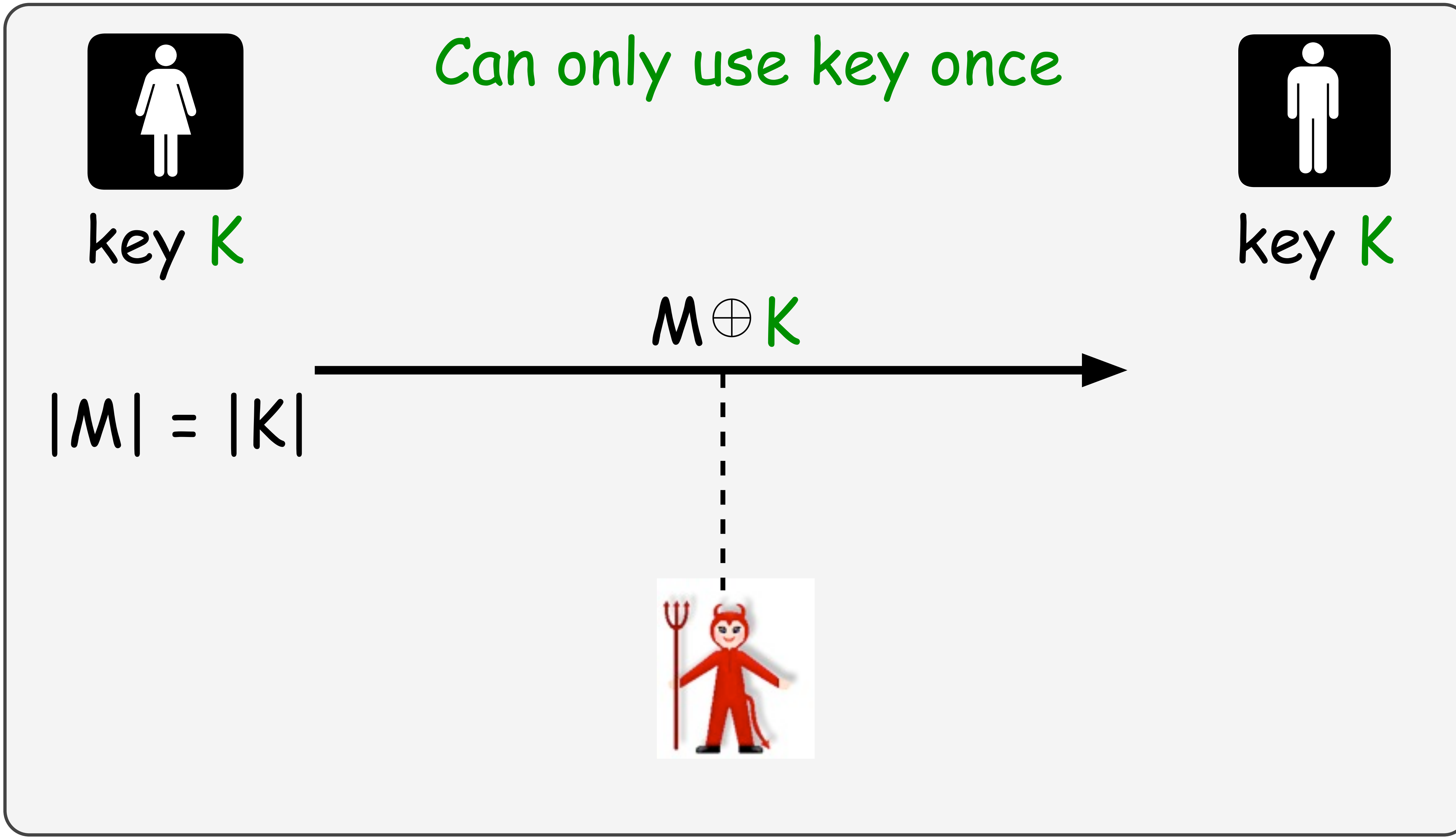
Cryptanalysis? Try all substitutions: $26! > 4.0 \times 10^{26}$.

Can cut down with probabilities of occurrence.



Example from D.R. Stinson (CRC Press)

One-Time Pad



Cryptanalysis? Perfectly secure ... but really expensive.

Diffie & Hellman's Vision

Whitfield Diffie

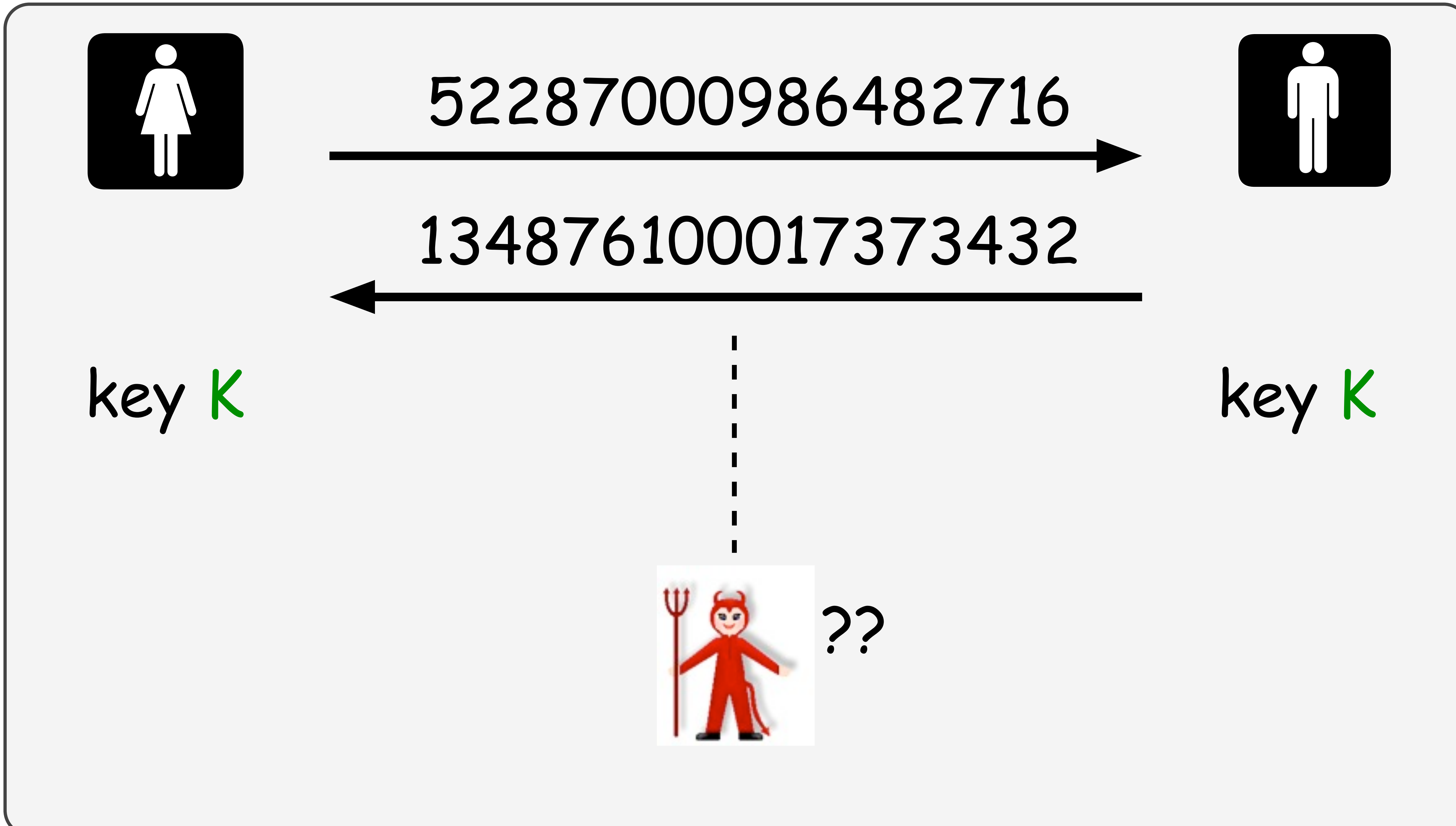
Martin Hellman

From "New Directions in Cryptography" 1976:

1. key exchange
2. public-key encryption
3. public-key signatures

Idea #1: Key Exchange

Setup shared secret K over insecure channel.



A Little Number Theory

Let Q be a large prime.

g generates a group G of order Q.

Example:

$Q = 3, g = 2, G = \{1, 2, 4\} \pmod 7$

$2^1=2 \quad 2^2=4 \quad 2^3=1 \pmod 7$

A Little Number Theory

We think the following problems are hard.

Discrete Log Problem:

Given (g, g^x) for random x, compute x.

Diffie-Hellman Problem:

Given (g, g^x, g^y) for random x, y, compute g^{xy}.

Decisional Diffie-Hellman (DDH) Problem:

Given (g, g^x, g^y, Q) for random x, y,
decide if $Q = g^{xy}$.

The DH Key Exchange

Setup shared secret K over insecure channel.

picks: (g, a)

key g^{ab}

$(g^b)^a = g^{ab}$

g, g^a →

← g^b

??

picks: b

key g^{ab}

$(g^a)^b = g^{ab}$

Open: given (g, g^a, g^b), quickly compute g^{ab}.

Diffie & Hellman's Vision

Whitfield Diffie

Martin Hellman

From "New Directions in Cryptography":

1. key exchange ✓
2. public-key encryption - ??
3. public-key signatures - ??

Inspiration

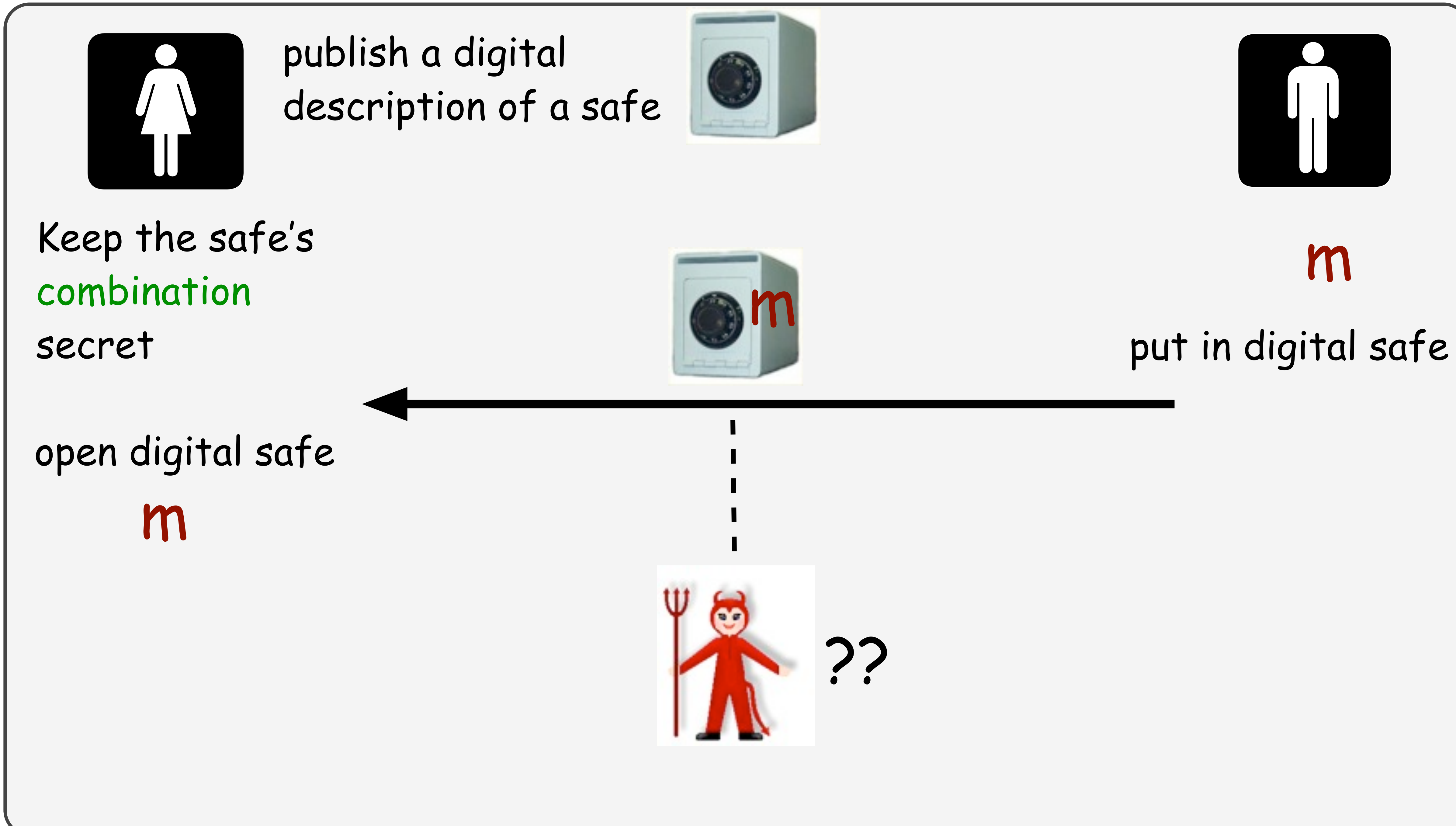
Observation about world:
It is sometimes asymmetric.

-- Easy to break vase,
hard to put it back together.

-- Anyone can close a safe,
but need the combination to open it.

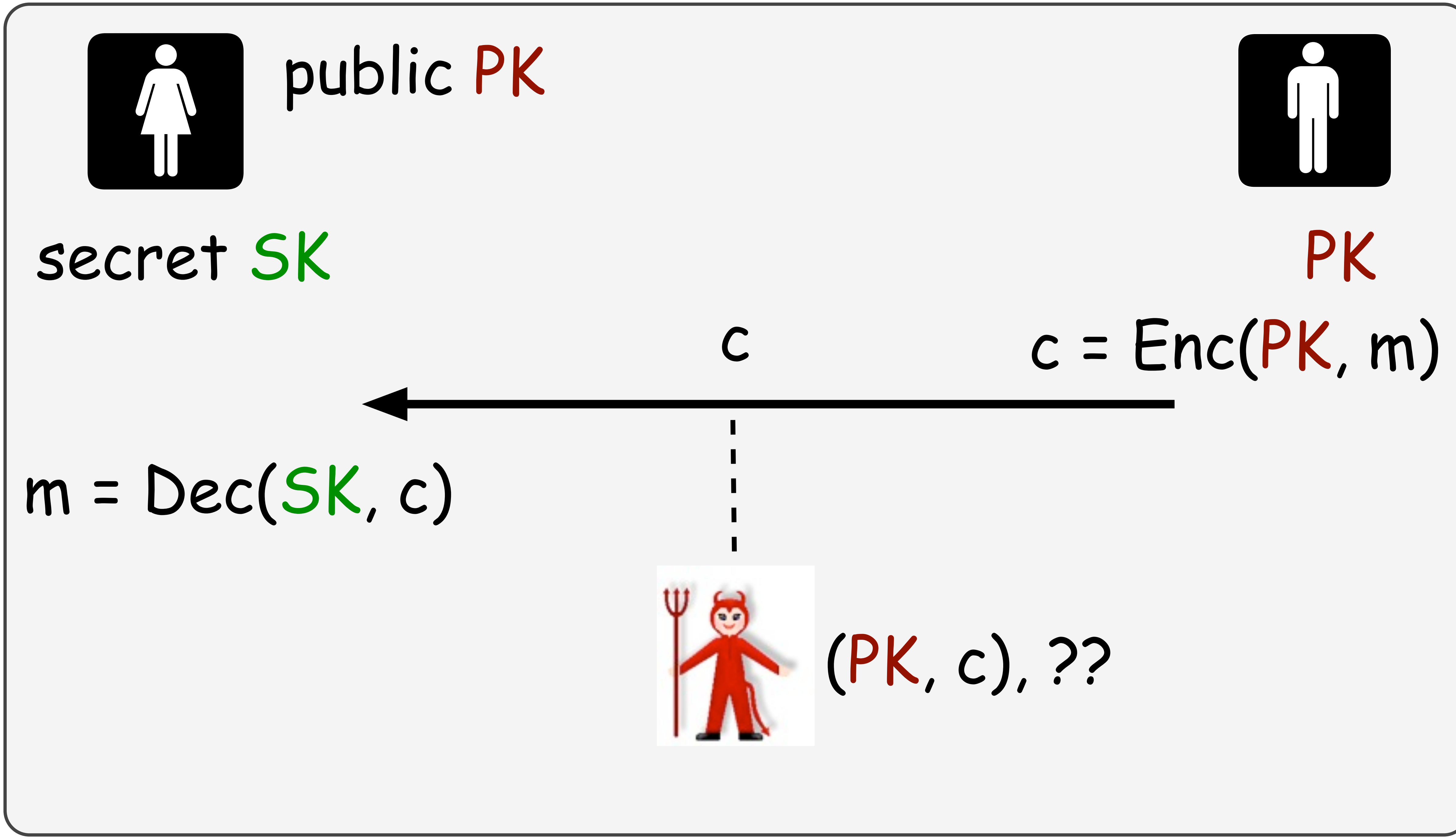
Idea #2: Public-Key Encryption

Encrypt without a shared secret.



Idea #2: Public-Key Encryption

Encrypt without a shared secret.



Idea #3: Digital Signatures

Dear Tal,

Do you want to go to a movie on Friday night?

--John

1976 Diffie-Hellman: dream of digital signatures

Idea #3: Digital Signatures

Dear Tal,

Do you want to
go to a movie on
Friday night?

--John

1adh84naf89hq32nvsd8
puwqhevhphvdfp9ufew7
u2rasdfohaqsedhfdasjf;

1976 Diffie-Hellman: dream of digital signatures

2000 Electronic Signatures in Global and National Commerce Act

Idea #3: Public-Key Signatures

Authenticate without a shared secret.

public PK

secret SK

PK

s = Sign(SK, m)

s →

Verify(PK, m, s) = 1

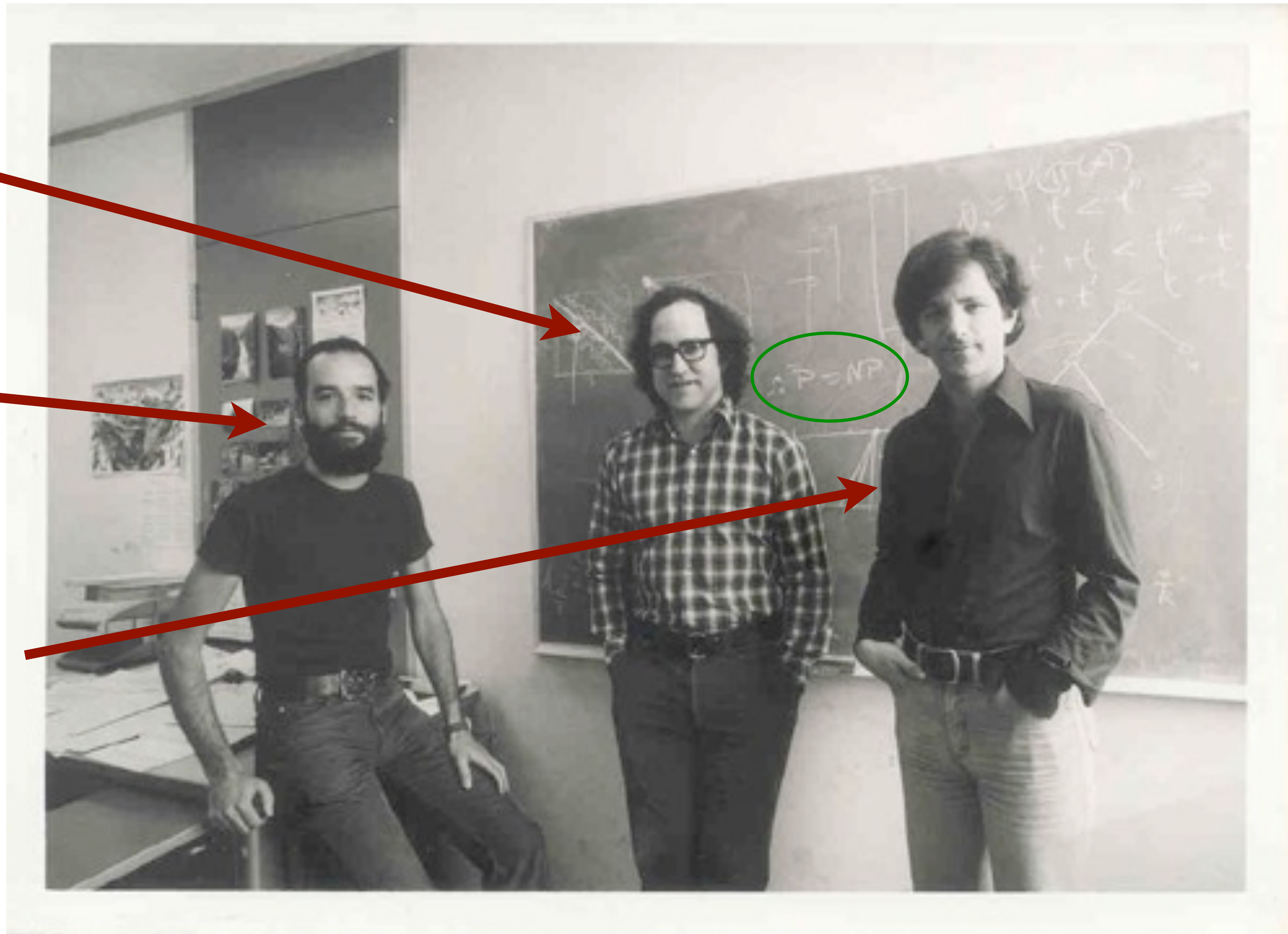
can't forge!

The RSA Realization (1978)

Rivest

Shamir

Adleman



The RSA Realization

Hard problem:

Let $N = pq$.

Given (N, y, e), find the x s.t. $e > 1$ and $y = x^e \bmod N$.

Public Key PK = (N, e)

Secret Key SK = d

Enc(N,e,m): $c = m^e \bmod N$	Sign(d,m): $s = m^d \bmod N$
Dec(d,c): $m = c^d \bmod N$	Verify(N,e,m,s): Accept iff $m = s^e \bmod N$

Is this "secure"?

Insecurity of textbook RSA

Enc(N,e,m): $c = m^e \bmod N$

Dec(d,c): $m = c^d \bmod N$

Sign(d,m): $s = m^d \bmod N$

Verify(N,e,m,s): Accept iff $m = s^e \bmod N$

Encryption: Can do a (small) dictionary attack.

Signatures: Given signatures on m1 and m2, can compute signature on m1m2.

Can Fix. But, what <u>exactly</u> do we mean by "secure"?

Goldwasser-Micali Definition

Encryption Security

PK →

Pick bit b.

c_b = Enc(PK, m_b)

← m_0 , m_1

c_b →

← b'

Pr[b=b'] <= 1/2 + a very small amount

El Gamal Encryption

Public Key: (g, g^a)

Secret Key: a

Enc(g, g^a, m):

1. pick a random k
2. $c1 = g^k$
3. $c2 = mg^{ak}$

$(c1,c2)$

Dec$(a, c1, c2)$:

1. $m = c2 / c1^a$

Secure if: given (g, g^a, g^b, Q), it is hard to decide if $Q=g^{ab}$.

Complexity Assumptions

Modern Crypto is built on number-theoretic assumptions.

Results look like:

Theorem: System X satisfies Definition Y under Assumption Z.

Technical Challenges:

1. Designing definitions that capture all attacks.
2. Creating systems.
3. Cryptanalysis of assumptions.

What else?

Next time we'll see something totally different:

zero-knowledge proofs.