Algorithms

Methods for securing communications

Michael L Perry
qedcode.com
@michaelllperry

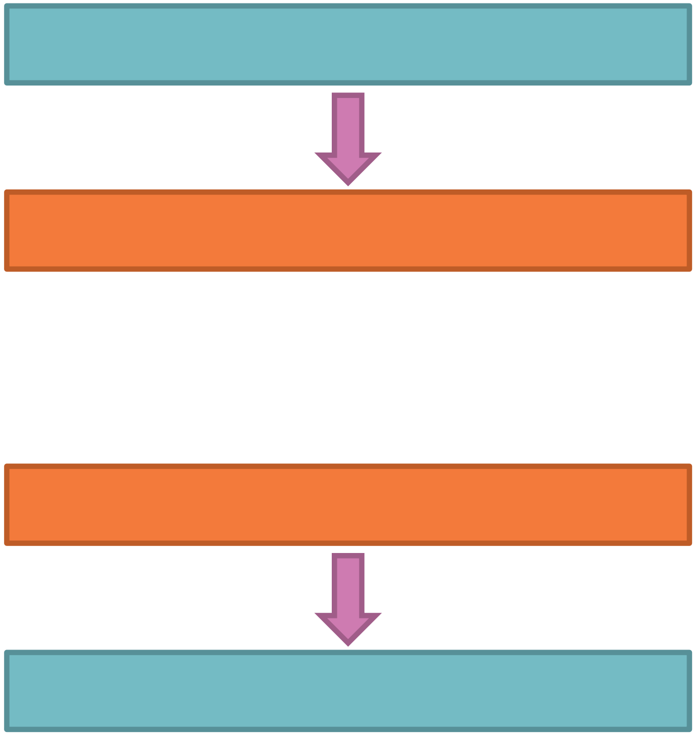
pluralsight
hardcore dev and IT training

Types of Cryptograph Algorithms

- **Symmetric**
- **Asymmetric**
- **Hash Functions**

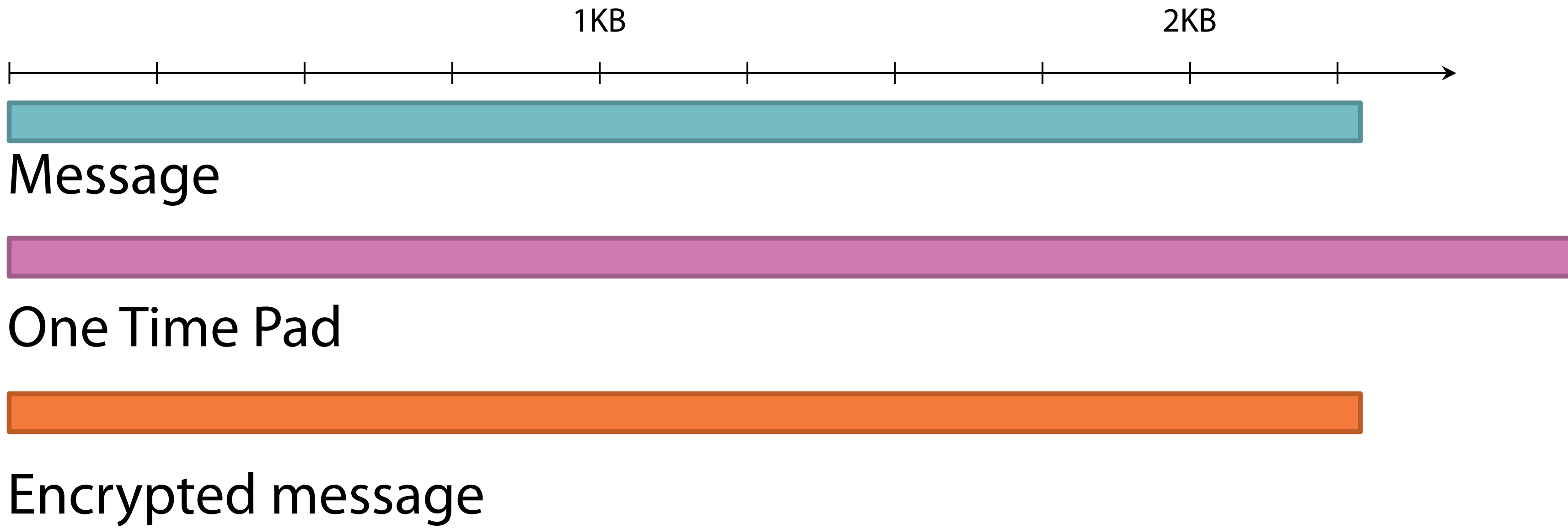
Cryptographic System

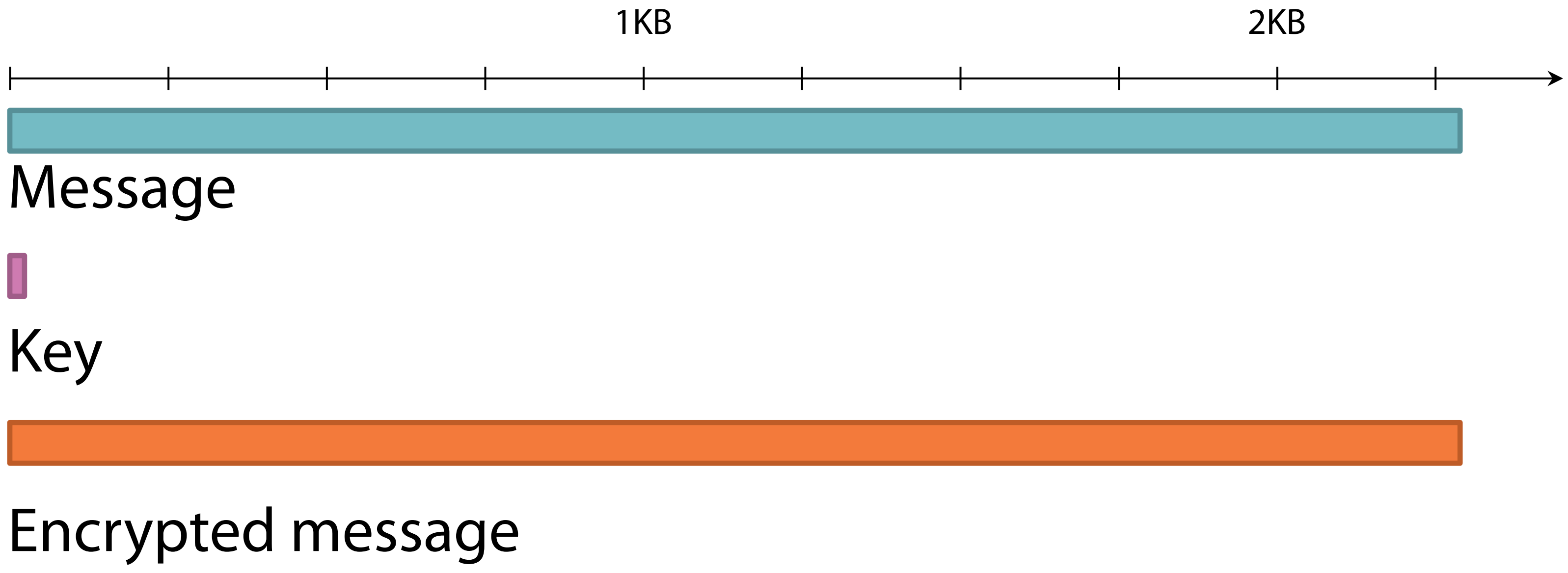
Symmetric Algorithms



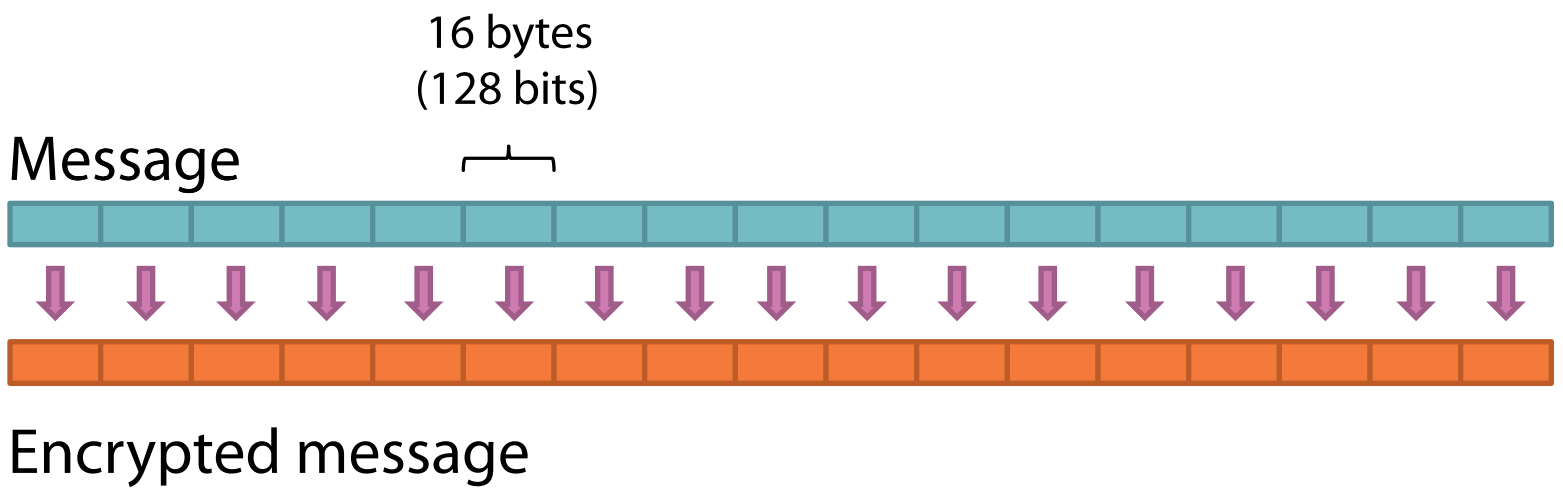
Encrypt

Decrypt

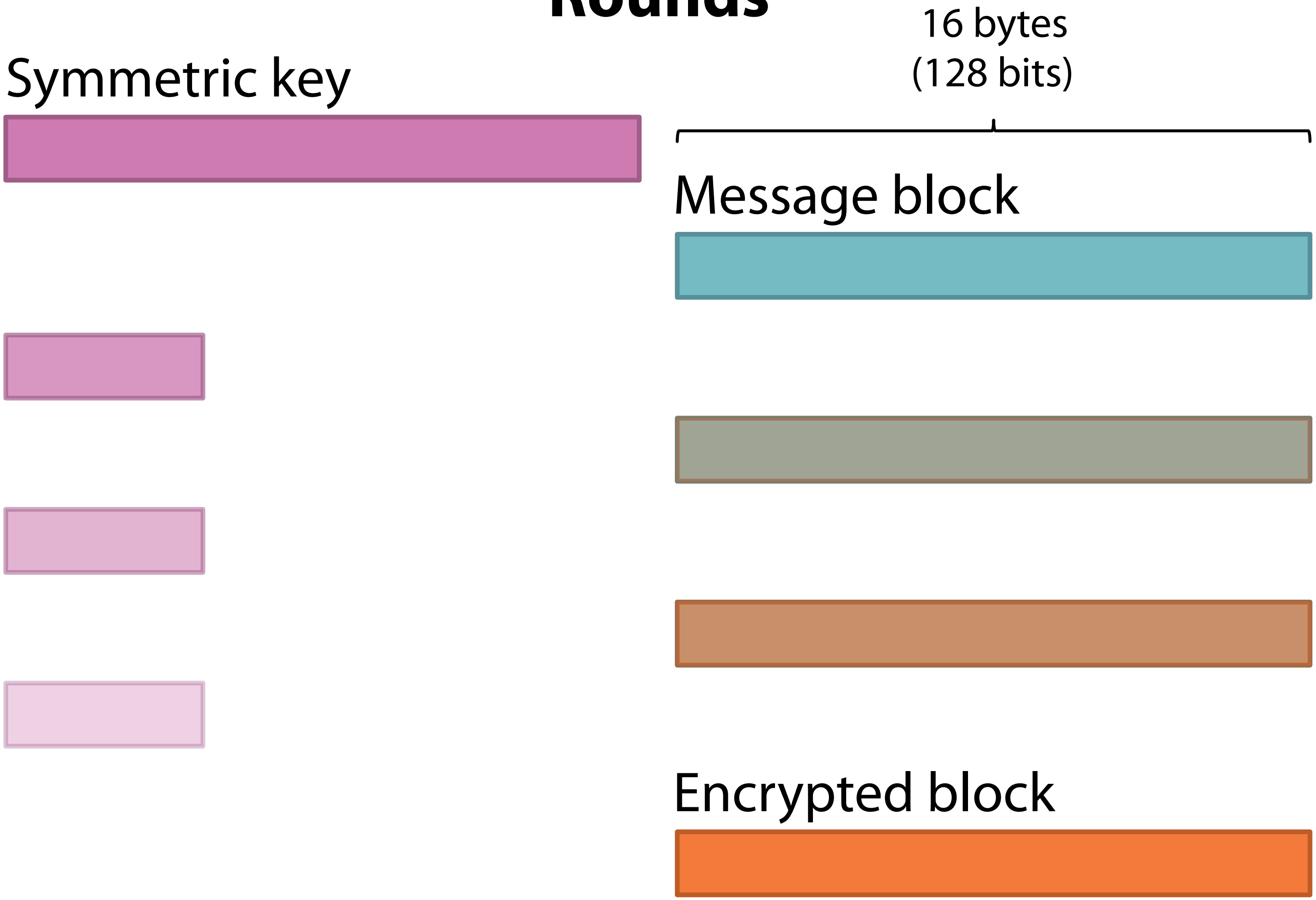

1KB
2KB
Message
One Time Pad
Encrypted message

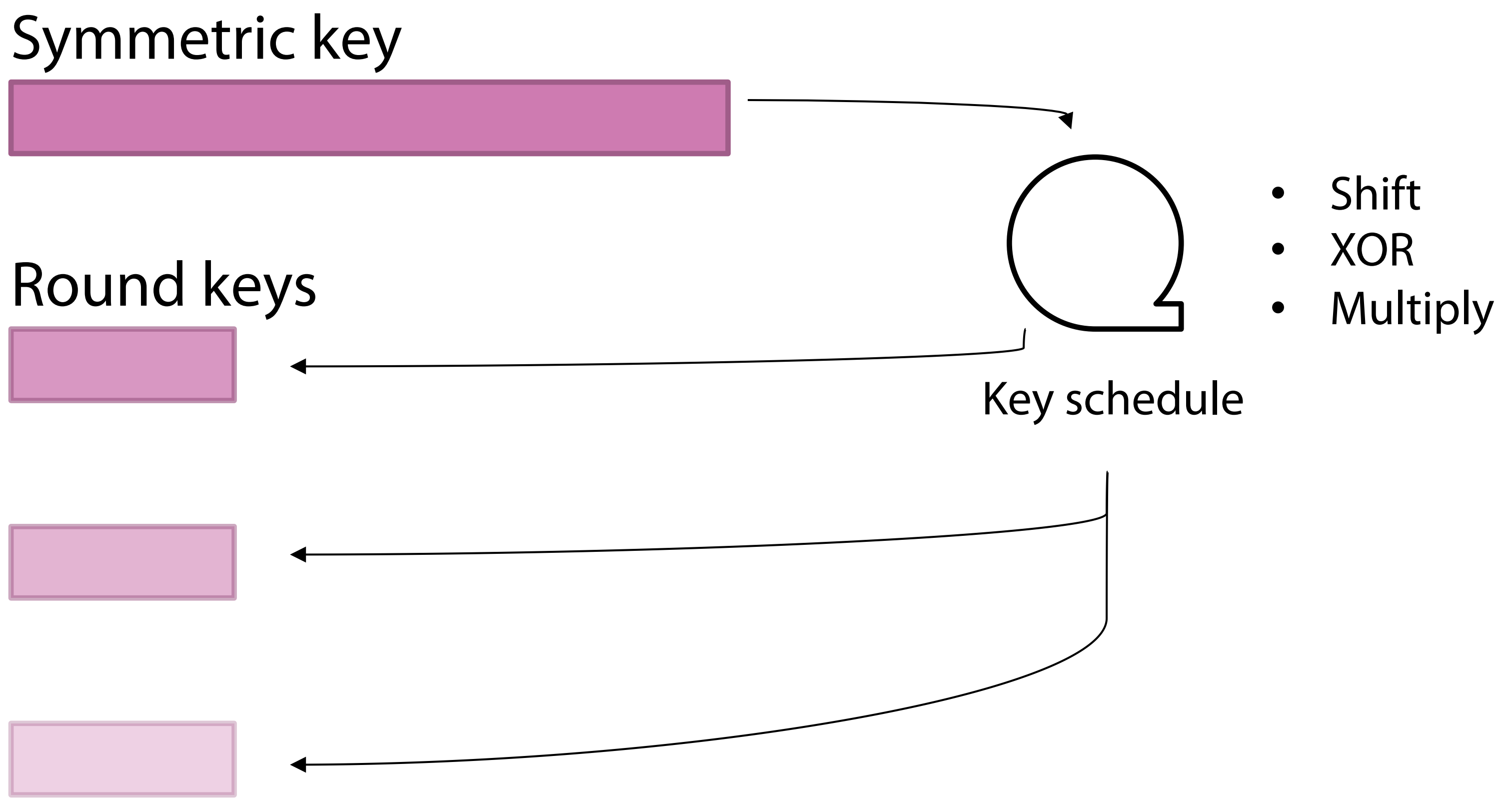

1KB
2KB
Message
Key
Encrypted message

Block Ciphers



Rounds


16 bytes
(128 bits)
Symmetric key
Message block
Encrypted block


Symmetric key
Round keys
Key schedule
• Shift
• XOR
• Multiply

Why Not XOR?

Message block

Symmetric key

Encrypted block

Claude E. Shannon

The Mathematical Theory of Communication

1948

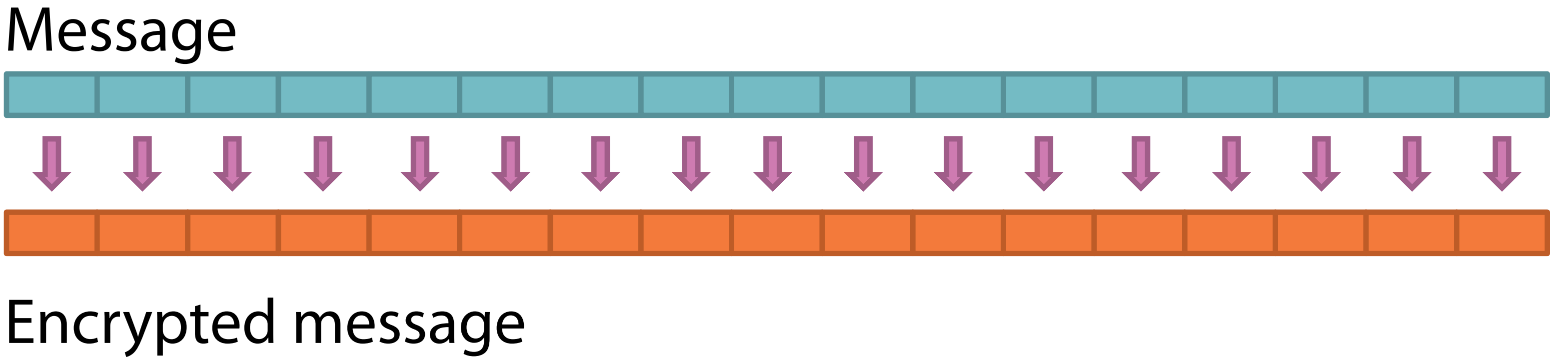
Communication Theory of Secrecy Systems

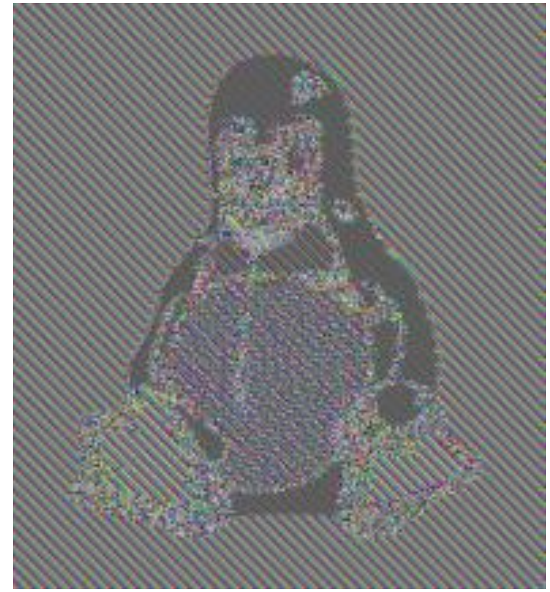
1949

Confusion and Diffusion

- **Confusion**
  - Relationship between key and ciphertext
  - Small change in key → large change in ciphertext
  - XOR is not sufficient; one-to-one
  - Key schedule
- **Diffusion**
  - Relationship between message and ciphertext

Electronic Code Book (ECB)

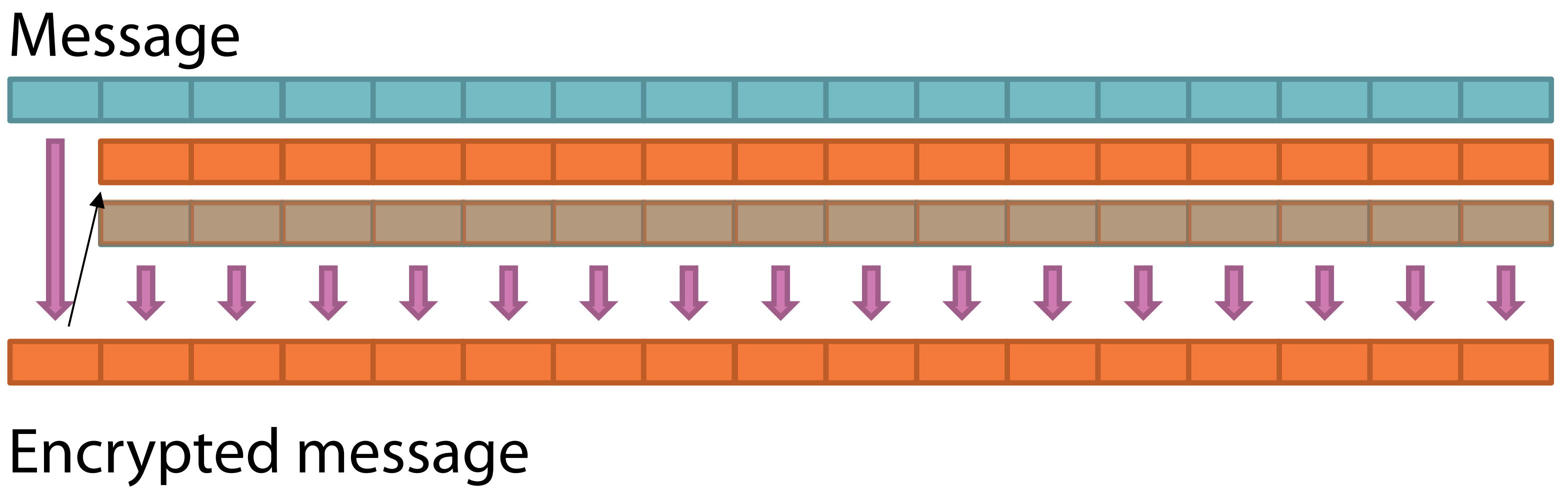


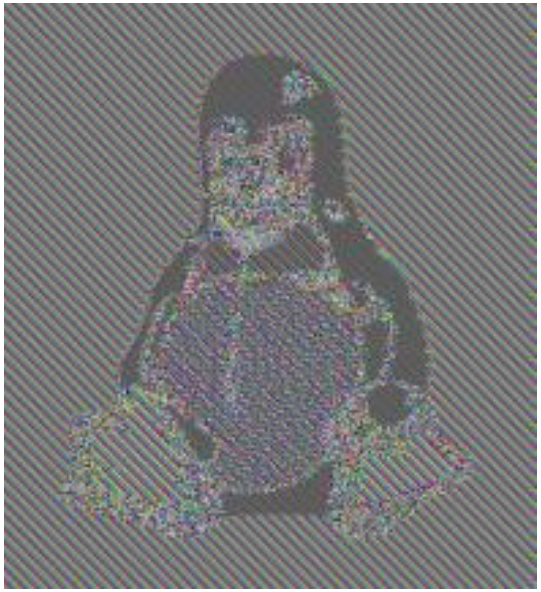
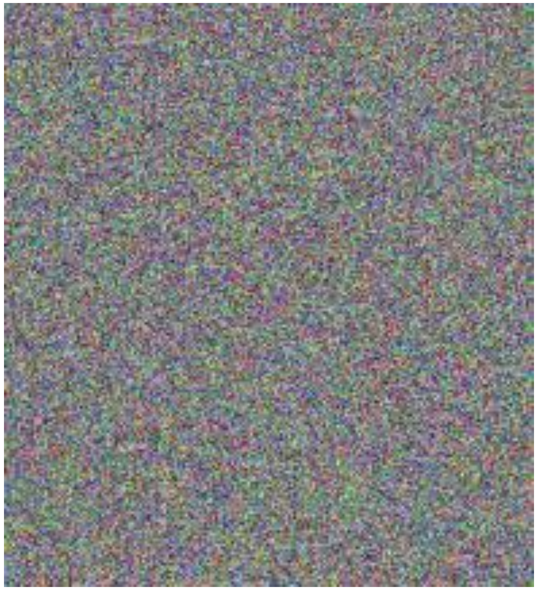


Diffusion

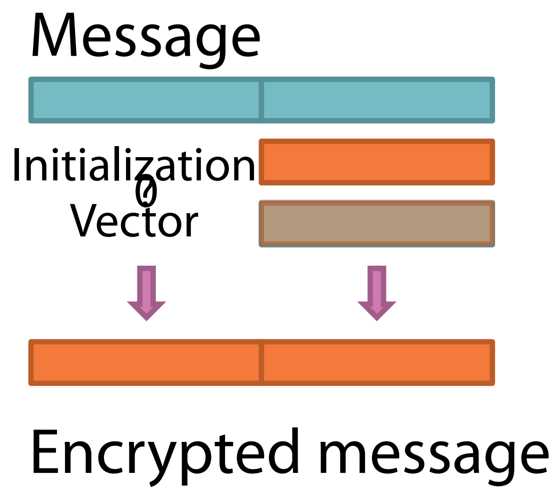
- Diffuse the information
- Small change in message → large change in ciphertext
- Hides patterns within the message

Cipher Block Chaining (CBC)



The First Block



GET http://qedcode.com/ HTTP/1.1
Host: qedcode.com

CBC with IV

- Diffuses information
- Encrypt message of arbitrary length
- Key of fixed length

Data Encryption Standard (DES)

Horst Feistel

IBM

1970s

Standardized

1977

Data Encryption Standard (DES)

- **Key length**
  - 64 bit input
  - 8 bit parity check
  - 56 bit effective key
- **Weaknesses**
  - Theoretical
  - Short key
- **3DES**
  - Run the protocol 3 times
  - Effective key length up to 168 bits
  - Slow

Encryption Standard Selection

National Institute of Standards and Technology (NIST)

1997 - 2000

Vincent Rijmen

Joan Daemen

Rijndael

Advanced Encryption Standard (AES)

- **Key lengths**
  - 128, 192, or 256 bits
- **Block size**
  - 16 bytes
- **Rounds**
  - Key expansion
  - XOR
  - Substitution
  - Shift rows
  - Mix columns

e3	37	90	2a
b3	77	2f	51
7c	de	3a	46
38	65	1f	2b

Key Expansion

- **Key schedule**
  - Shift
  - XOR
  - Multiply
- **Confuses key**
- **16 byte round key**
- **XOR key with message block**

S-Box

- Substitution box
- Lookup table

63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Shift Rows and Mix Columns

e3	37	90	2a
b3	77	2f	51
7c	de	3a	46
38	65	1f	2b

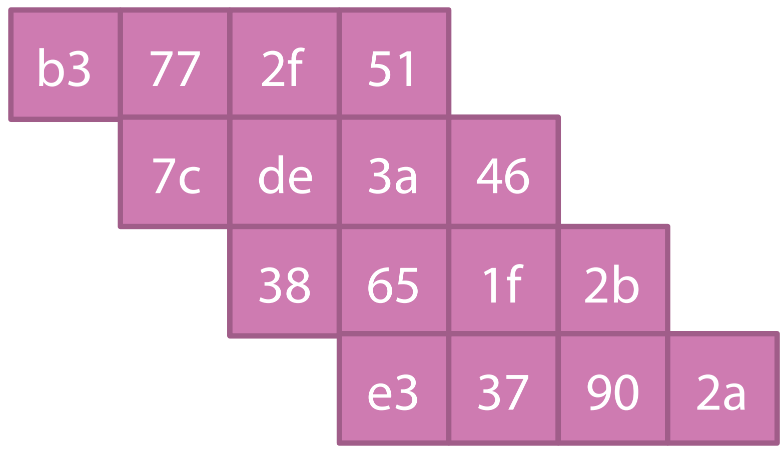
Shift Rows and Mix Columns

b3	77	2f	51
7c	de	3a	46
38	65	1f	2b
e3	37	90	2a

Shift Rows and Mix Columns

b3	77	2f	51
7c	de	3a	46
38	65	1f	2b
e3	37	90	2a

Shift Rows and Mix Columns



Shift Rows and Mix Columns

b3	77	2f	51
46	7c	de	3a
1f	2b	38	65
37	90	2a	e3

Further confuses key

Recommendations

- **AES-256**
  - Top Secret level
  - Provides confusion
- **Cipher Block Chaining**
  - Provides diffusion

Modern Cryptanalysis

- **Enigma**
  - 47.1 bits in plug board
  - 4.7 x 3 = 14.1 bits in rotors
  - Total 61.2 - 64 bits

  - No memory
    - Hence, no diffusion
  - Predictable key changes
    - Hence, little confusion

- **AES**
  - 128 - 256 bits of entropy
- **DES**
  - 56 bits

  - CBC and IV
    - Good diffusion
  - Rounds
    - Good confusion

Compression

- **Information content of English text**
  - 0.6 to 1.3 bits of information per character
  - Redundancy
  - Patterns
  - Predictable
- **Compressed ASCII**
  - Theoretical limit: 7.5% to 16% of size
  - In practice: 40% of size
  - Squeezes out redundancy
  - Preserves information
- **Compressed ZIP**
  - Ineffective
  - Patterns are already removed

Encryption vs Compression

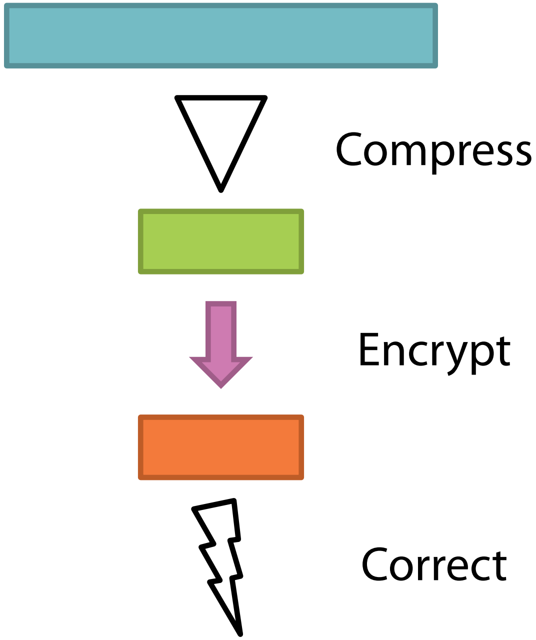
- **Encryption**
  - Masks patterns
  - Adds information
  - Compression after encryption is not effective
- **Compress before encrypt**
  - Compression uses redundancy
  - Compression removes patterns
  - Smaller message
  - More diffused

Error Correction

- **Operation**
  - Checksums
  - Discover errors
  - Correct errors
- **Combined with encryption**
  - Adds redundancy
  - Easier to crack
- **Correct at time of transmission**
  - Does not weaken encryption
  - Just as effective

Benefits of Information Theory

- Compression
- Error Correction
- Encryption



Asymmetric Algorithms

- **Diffie-Hellman**
  - Vulnerable to man-in-the-middle attacks
- **Proof of identity**
  - Means of identification — Public key
  - Method of proof — Private key

Pair of Functions

$f(x)$	$f^{-1}(x)$
Function	Inverse

Inverse Functions

Message	m	
Cyphertext	$f(m) = c$	Public key
	$f^{-1}(c) = m$	Private key

Exponentiation in a Modulus

- **Jumps around**
  - Hard to find the root
  - Easy to find the exponent
- **Make up two functions**
  - Encrypting exponent (e)
  - Modulus (n)
  - Decrypting exponent (d)

$$m^e = c_{\ (\mathrm{mod}\ n)}$$

$$c^d = m_{\ (\mathrm{mod}\ n)}$$

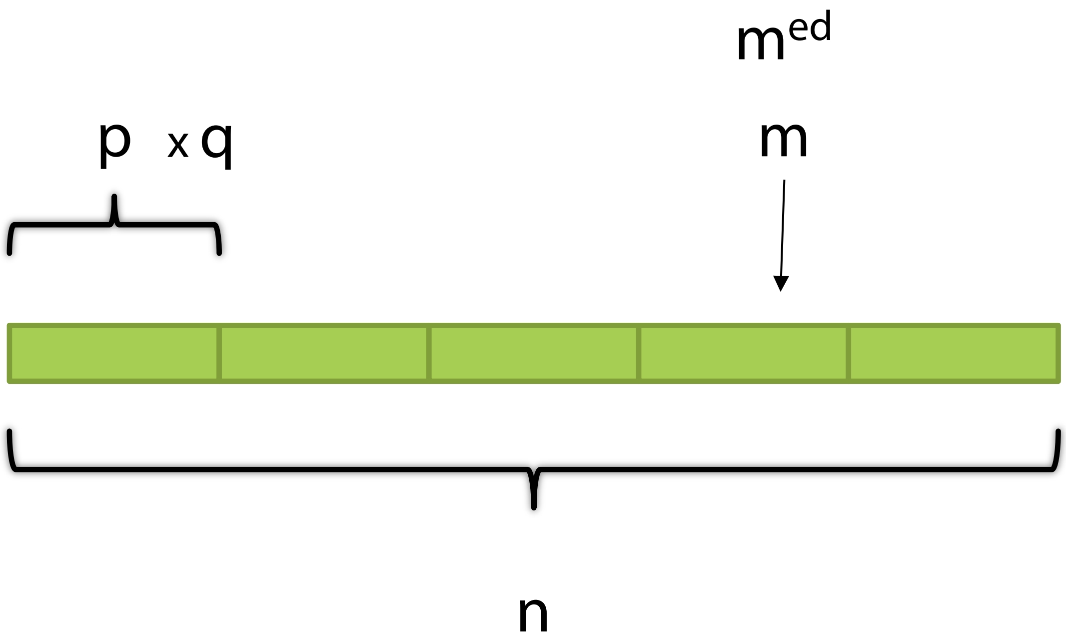
$m^e = c_{\text{(mod n)}}$ $c^d = m_{\text{(mod n)}}$

$$(m^e)^d = m \ _{(\mathrm{mod}\ n)}$$

$$m^{ed} = m \pmod{n}$$

$$m^{ed} = m \pmod{n}$$

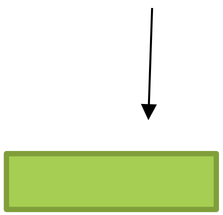
$$\begin{array}{ccc} 77 & 7 & 11 \\ n & = p & q \end{array}$$



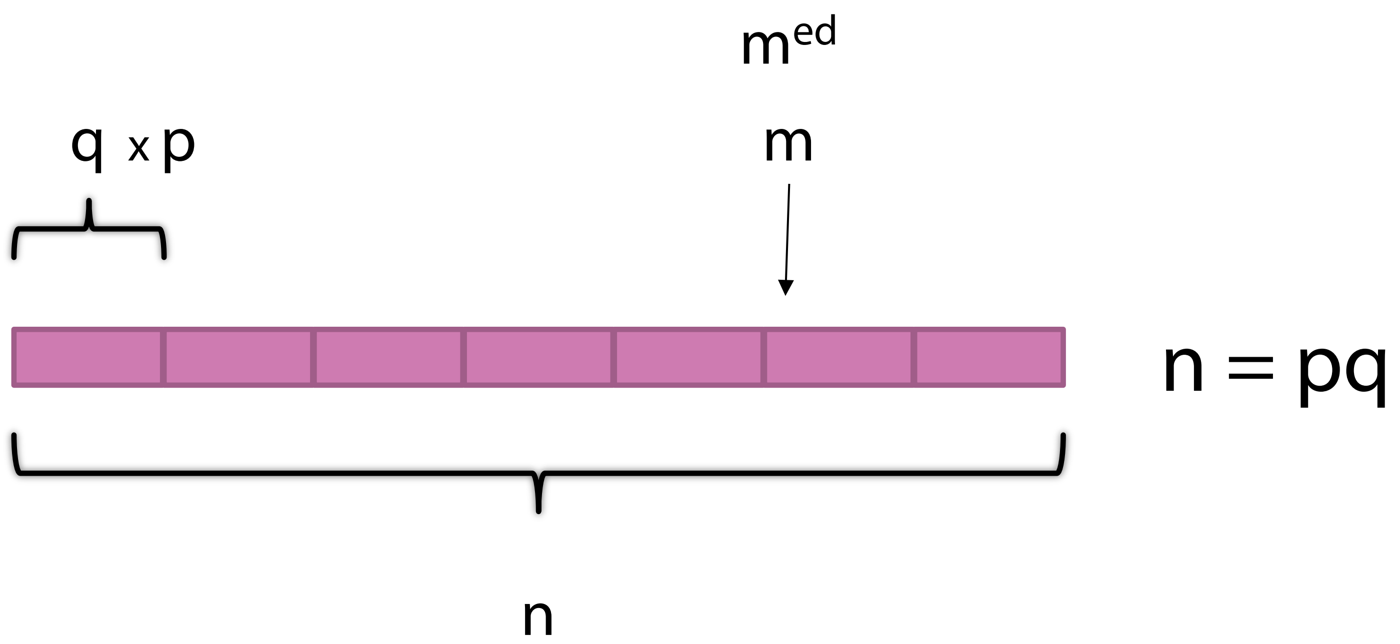
$$n = pq$$

m^{ed}

m



$n = pq$



m^{ed}
$q \times p$
m
$n = pq$
n

m^{ed}

m

$$n = pq$$

$m^{ed} = m_{\text{ (mod p)}}$ $m^{ed} = m_{\text{ (mod q)}}$ $n = pq$

$$m^{ed} = m_{\text{ (mod p)}}$$

$$n = pq$$

$$m?^{(ed-1)} = 1 \qquad m$$

$$m^{(ed-1)}\, m = m_{\ (\mathrm{mod}\ p)}$$

$$n = pq$$

$$m^{(p-1)} = 1_{\ (\mathrm{mod}\ p)}$$

$$ed - 1 = h(p-1)$$

$$(m^{(p-1)})^h m = m \pmod{p}$$

$$n = pq$$

$$ed - 1 = h(p-1)$$

$$(1)^h m = m_{\pmod p}$$

$$n = pq$$

$$ed - 1 = h(p-1)$$

$1\,m = m_{\text{(mod p)}}$

$n = pq$

$ed - 1 = h(p-1)$

$$m^{ed} = m \pmod{q}$$

$$n = pq$$

$$ed - 1 = h(p-1)$$

$m^{ed} = m \pmod{q}$

$n = pq$

$ed - 1 = h(p-1)(q-1)$

13 37 7 11

481 6 10

480 8 60

Suitable Numbers

$$n = pq$$

$$ed - 1 = h(p-1)(q-1)$$

Fermat's Little Theorem

$$g^{(p-1)} = 1_{\ (\text{mod } p)}$$

$g = 2, 3, 4, 5, \ldots$

Primality test

Choosing Numbers

Choose p and q prime

$$n = pq$$

Choose e having
no common factor with $(p-1)(q-1)$

$$ed - 1 = h(p-1)(q-1)$$

13 37 60

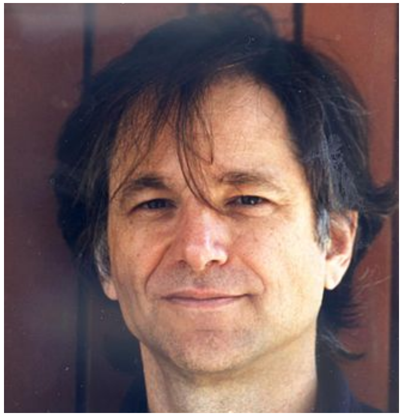
Extended Euclidean Algorithm

Chosen Keys

$$f(m) = m^{13} \pmod{77}$$ Encrypt

$$f^{-1}(c) = c^{37} \pmod{77}$$ Decrypt

RSA Algorithm



1977

Ron Rivest

Adi Shamir

Leonard Adleman

1973

Clifford Cocks

Discrete Logarithm Problem

Inverse of exponentiation within a modulus

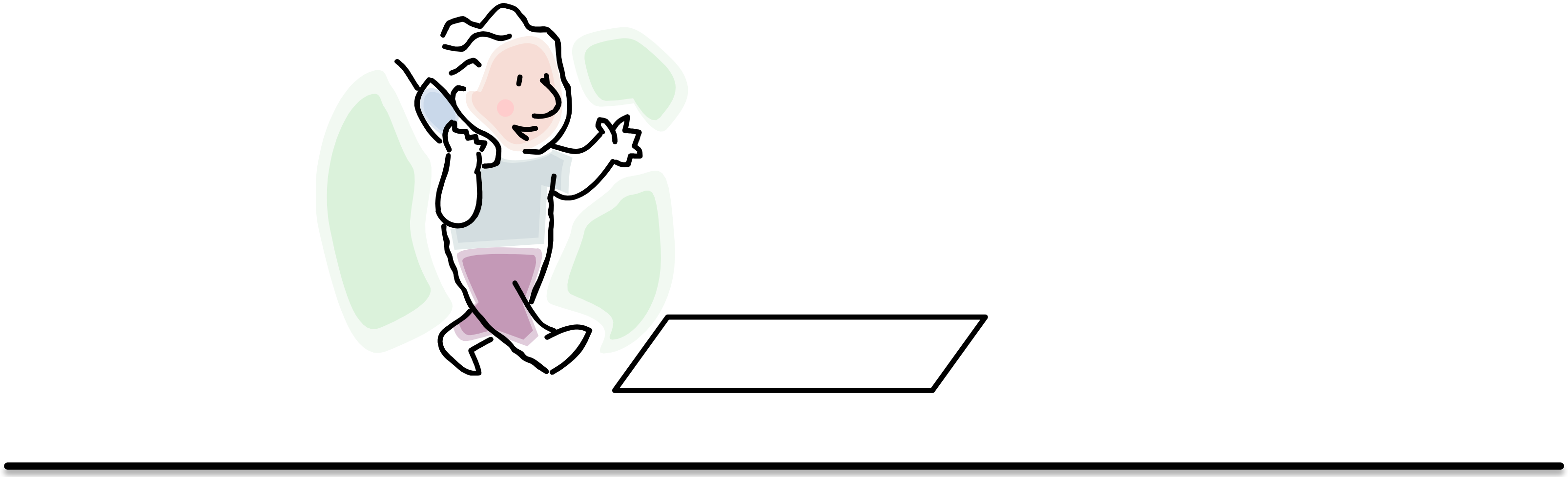
Given:

m^e (mod n) $\quad m \quad n$

Find:

e

Trapdoor Function



Big O Notation

Express work as a function of input

Search	$O(\log n)$	$\log 2n = (\log n) + 1$
Scan	$O(n)$	$2n = 2\ (n)$
Sort	$O(n \log n)$	$2n \log 2n = 2\ (n \log n) + 2n$

Big O of Discrete Logarithm Problem

$$m^e \ (\text{mod } n)$$

Try every e

b = number of bits

$$O(2^b)$$

$$2^{(2b)} = (2^b)^2$$

A Heuristic Quasi-Polynomial Algorithm for Discrete Logarithm in Finite Fields of Small Characteristic

March 2014

Razvan Barbulescu
Pierrick Gaudry
Antoine Joux
Emmanuel Thomé

$$n = q^{2k}$$

for $q \approx k$

quasi-polynomial

$b^{O(\log b)}$

$2b^{\log 2b} = (b^{\log b})\ 2b$

as q and k diverge

approaches exponential

if

$$n = q^{2k}$$

then

m^e $_{(\mathrm{mod}\ n)}$ is not a trapdoor

Diffie-Hellman	n is prime
RSA	$n = pq$

Diffie-Hellman and RSA are Safe

(for now)

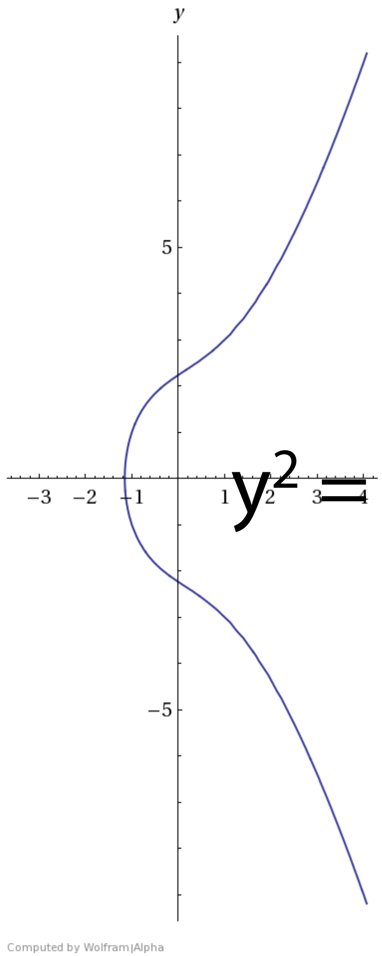
Elliptic Curve Cryptography

Neal Koblitz

Victor S. Miller

1985

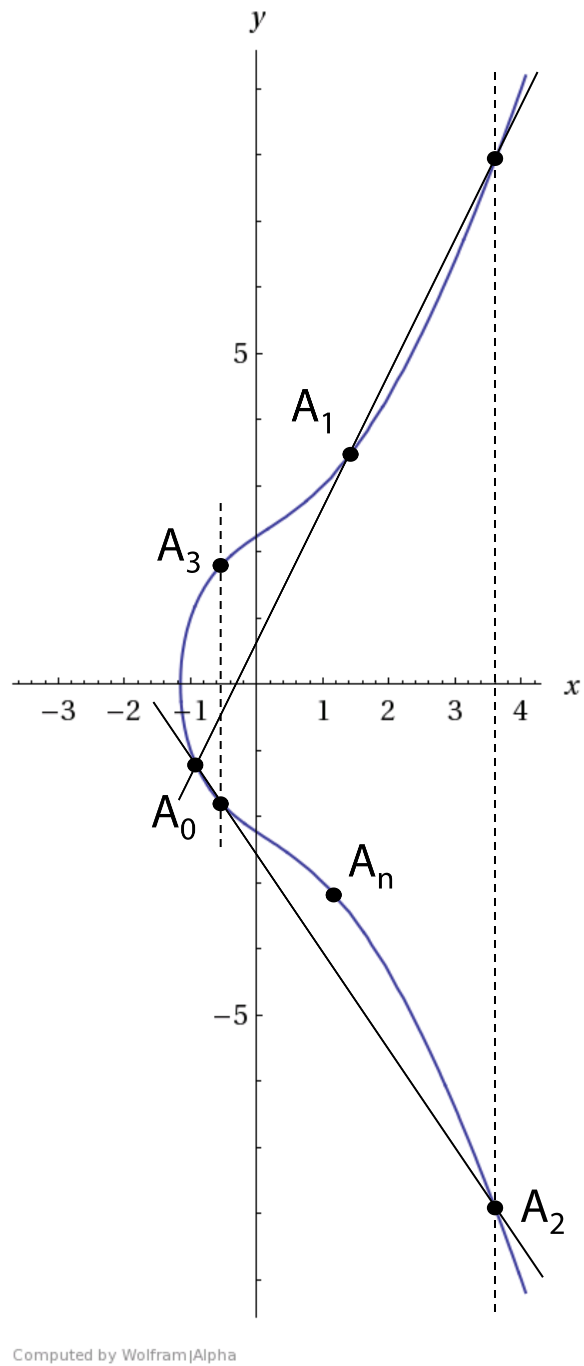
Elliptic Curve Equation



$$y^2 = x^3 + 3x + 5$$

Properties of Elliptic Curves

- A non-vertical line intersecting 2 points also intersects a third
- No line intersects at more than 3 points
- The curve is symmetrical


y
x
5
−5
−3
−2
−1
1
2
3
4
A1
A3
A0
An
A2
Computed by Wolfram|Alpha

Two Functions

- **Given A_0, A_1, n**
  - Find A_n
  - Easy (ish)
- **Given A_0, A_1, A_n**
  - Find n
  - Good luck!
  - Run each iteration until you hit A_n

Public/Private Key Pair

- **x and y**
  - Integers
  - Prime modulus

$$y^2 = x^3 + 3x + 5 \pmod{p}$$

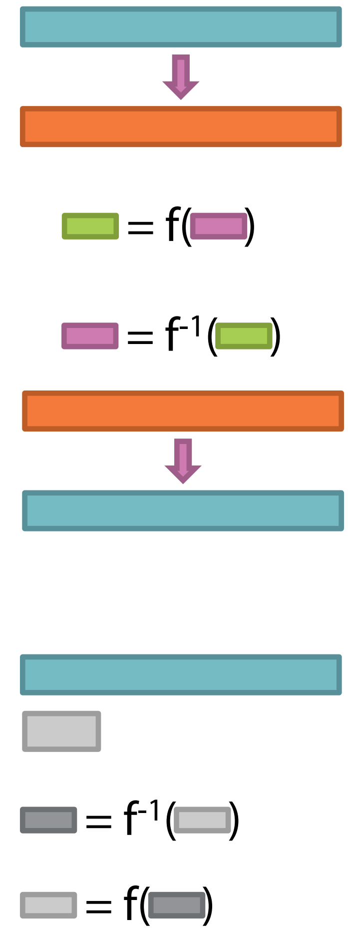
- **Private key (n)**
- **Public key (A_n)**

Key Lengths

- **ECC (Elliptic Curve Cryptography)**
  - 163 – 359 bits ($\approx 10^{49}$ - 10^{108})
- **RSA**
  - 2048 bits ($\approx 10^{616}$)

Use of Algorithms

- **Confidentiality**
  - Encrypt a message
  - Encrypt symmetric key with public key
  - Confidence that only recipient can read it



- **Authenticity**
  - Guarantee the source
  - Digest of message (hash)
  - Encrypt digest with private key (signature)
  - Compute same hash
  - Decrypt signature with public key

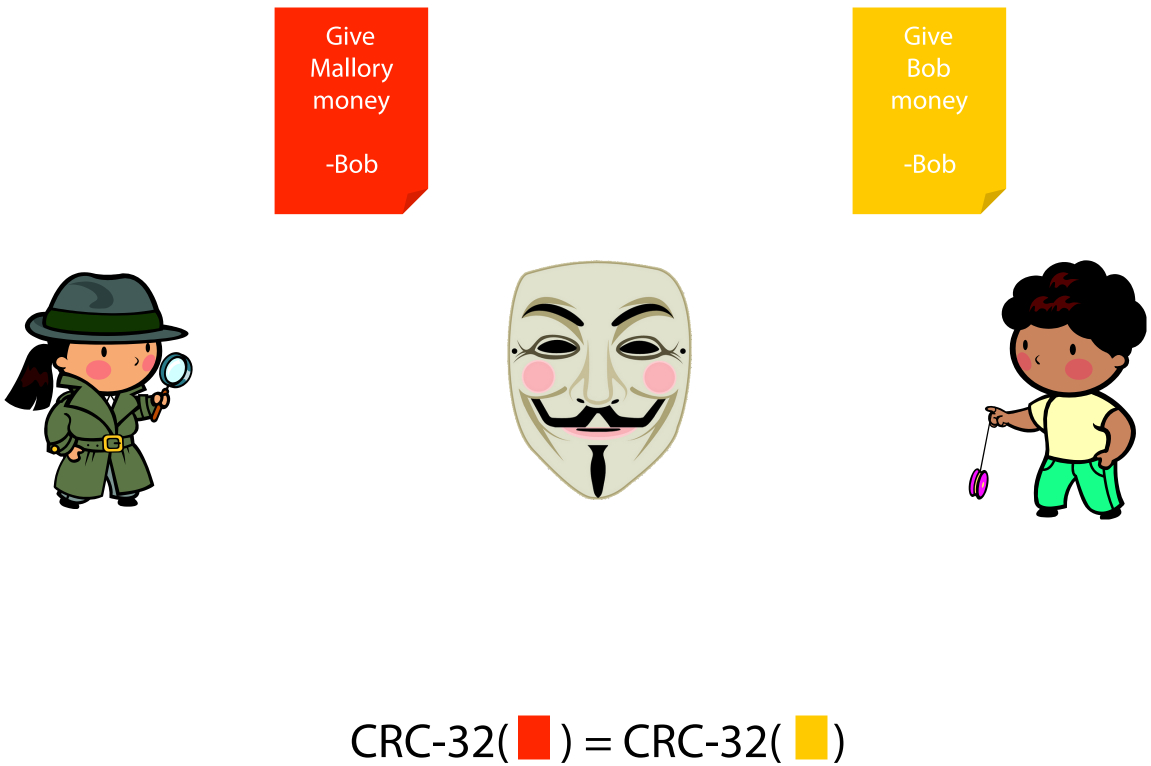
CRC-32

- **Cyclic Redundancy Check**
- **32-bit hash**

$$x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^{8} + x^{7} + x^{5} + x^{4} + x^{2} + x + 1 \ _{(\text{mod } 2^{33})}$$

- **Easily reversible**
- **Intended for error detection**
- **Not appropriate for digital Signatures**

Weakness of CRC-32



Cryptographically Strong Hashing Algorithms

Ralph Merkle

Ivan Damgård

Bit shifts, modulus addition, XOR in rounds

Diffuse message

MD5

- Severe weaknesses
- No longer suitable

SHA-1

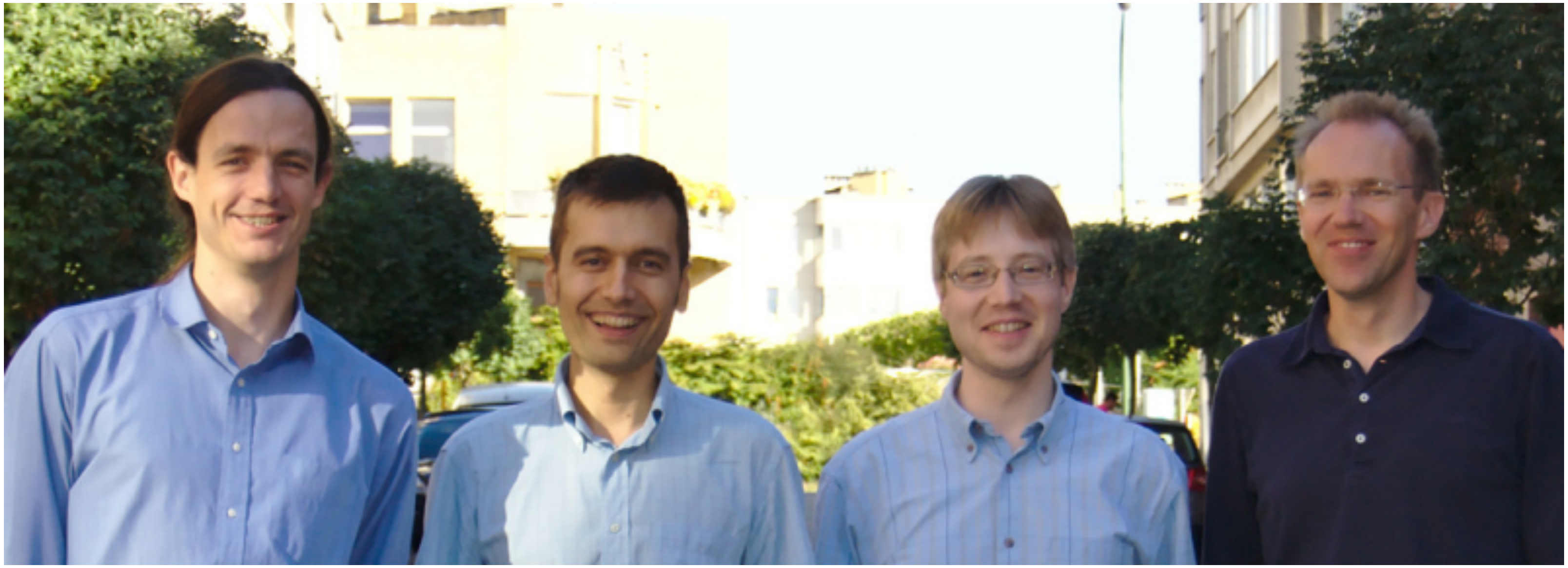
- 160 bit hash
- NSA
- Found weaknesses
- No longer recommended after 2010

SHA-2

- **NSA**
- **Family**
  - SHA-256
  - SHA-512
- **New functions**

SHA-3

- **2012 NIST**
- **Keccak**



Michaël Peeters Guido Bertoni Gilles Van Assche Joan Daemen

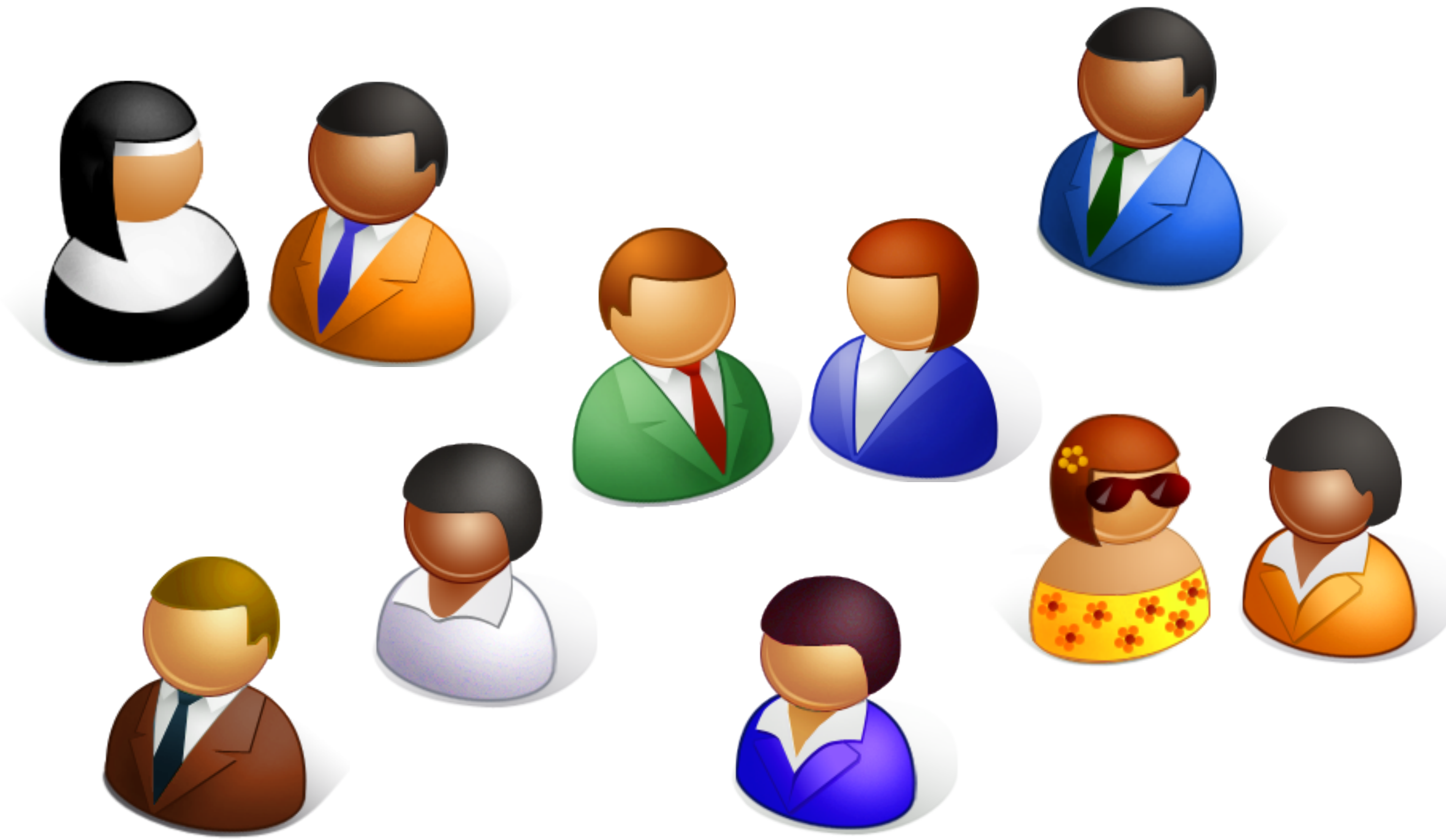
- **224 – 512 bit hash**
- **More internal state**


Give
Mallory
money

-Bob
Give
Bob
money

-Bob

The Birthday Attack



Probability that two share a birthday

= 1 – everybody has unique birthday

1

365/365

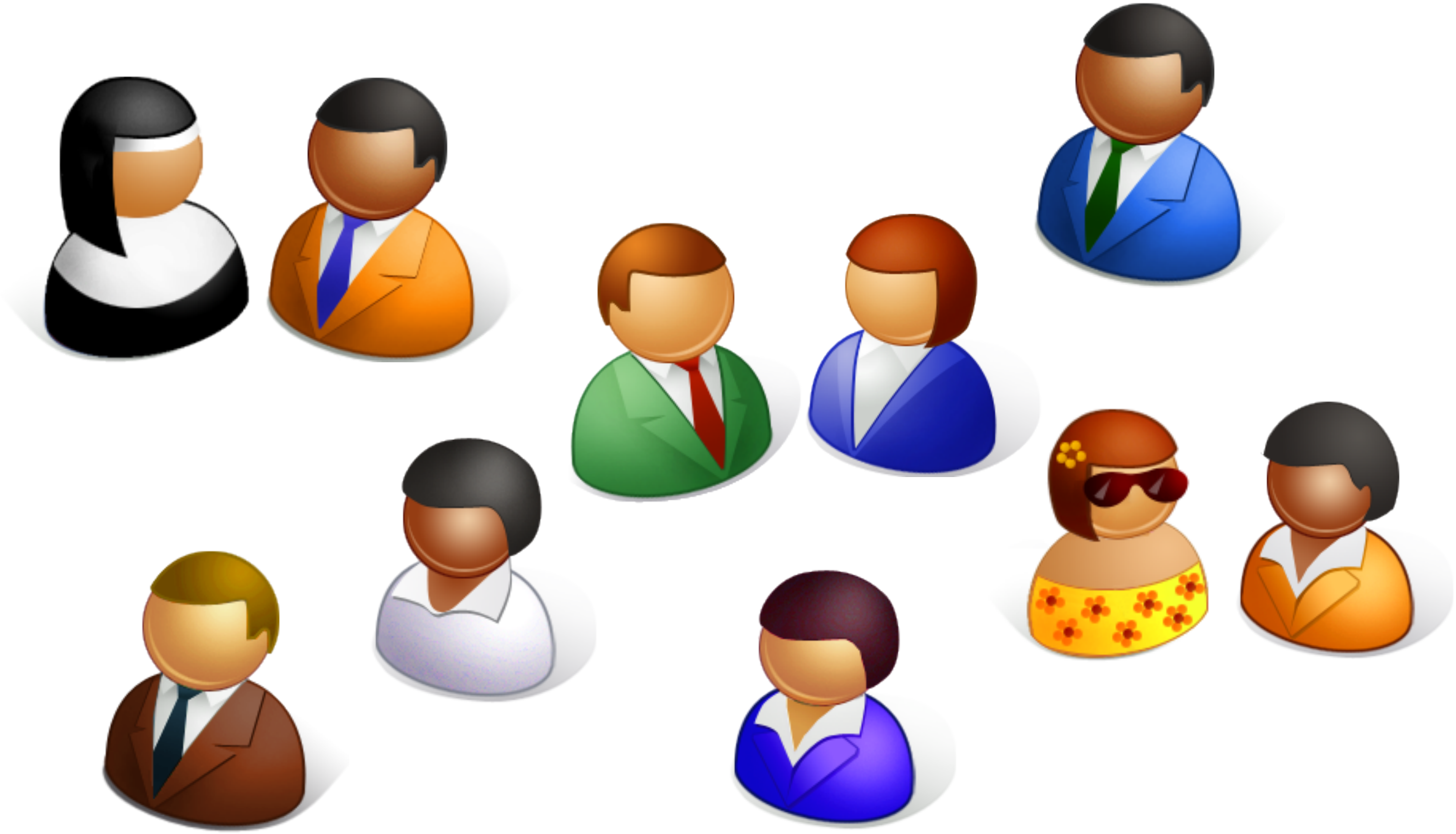
364/365 99.7%

99.4%

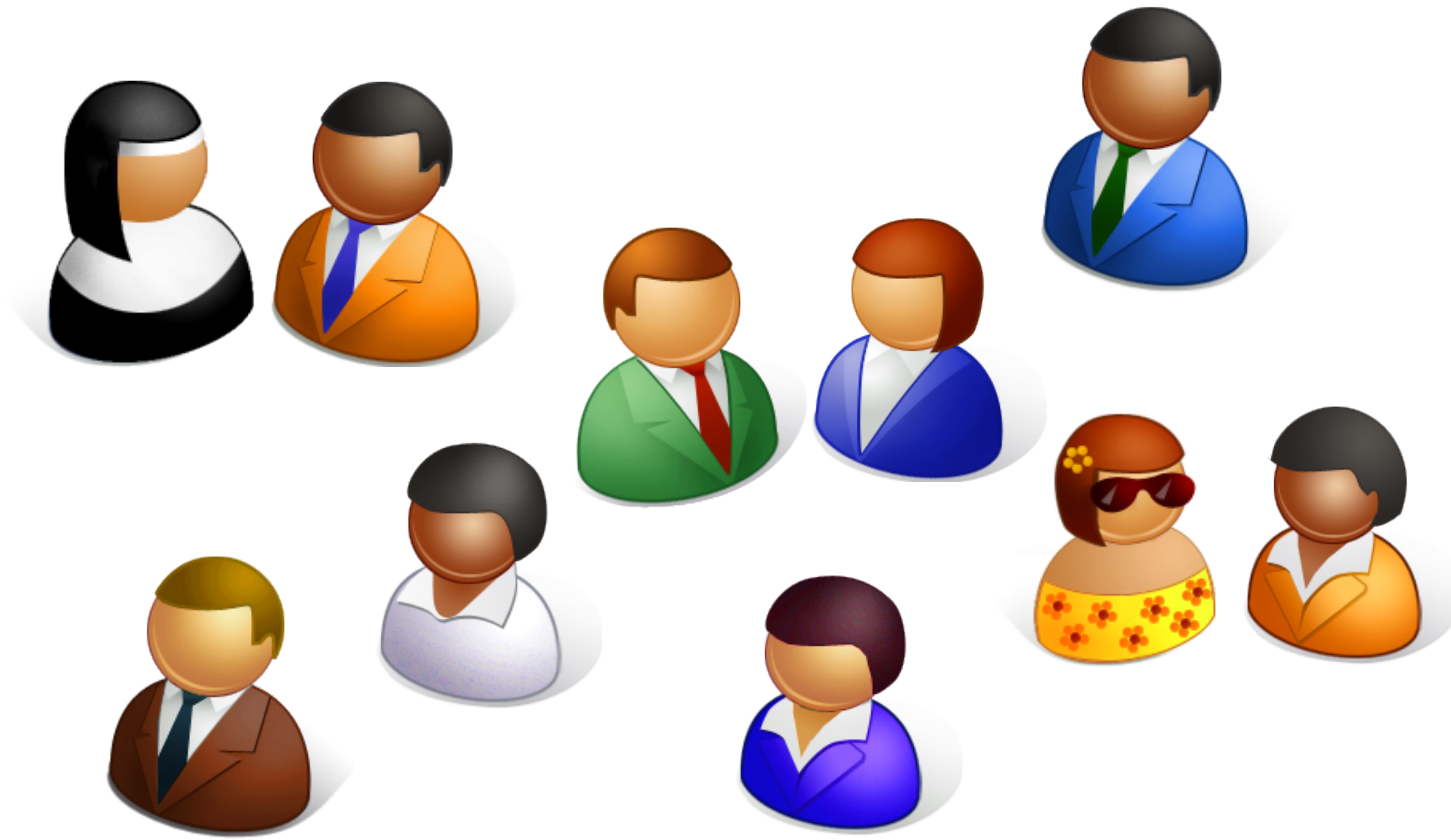
363/365

365/365

364/365



346/365 94.7%



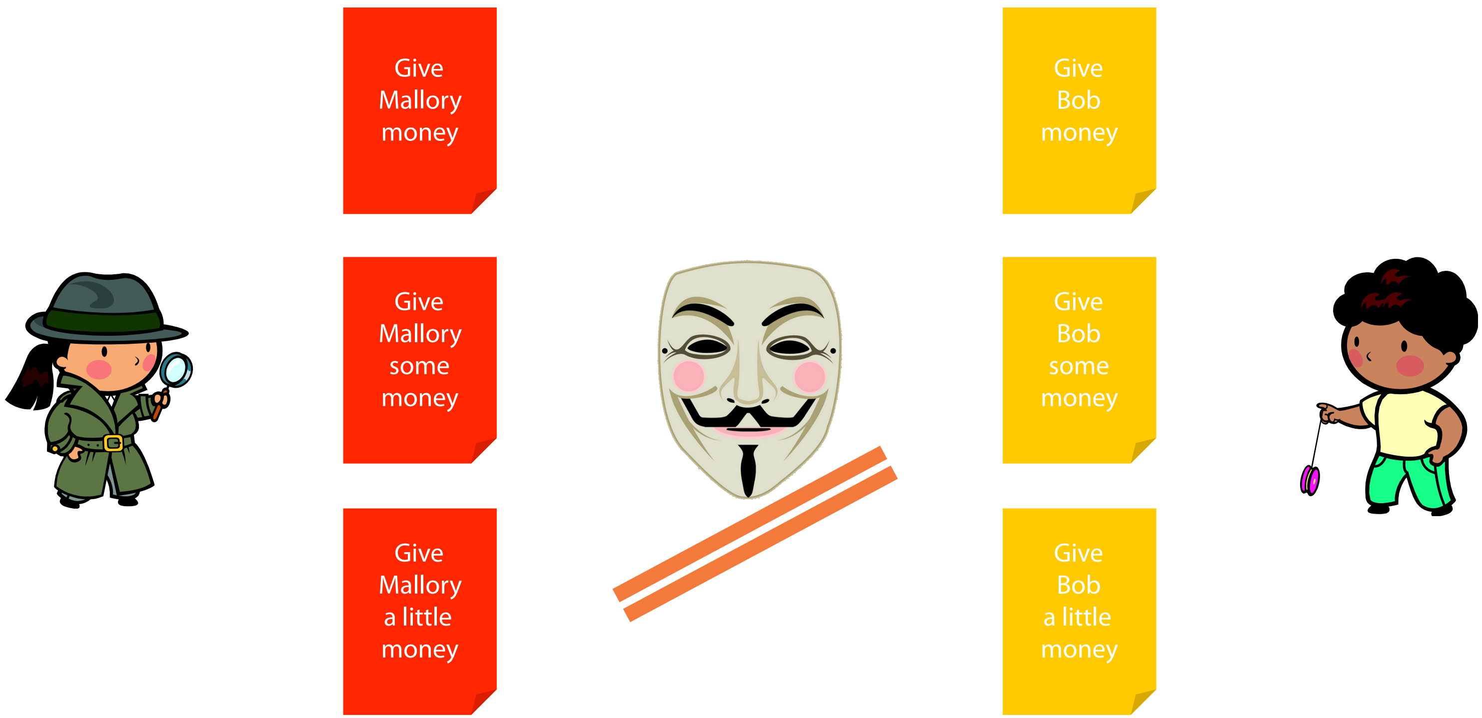
$$365/365 \times 364/365 \times 363/365 \times \cdots \times 346/365 = 58.9\% = 1 - 41.1\%$$

With 23 people,

the probability of two sharing a birthday

is greater than 50%

The Birthday Attack



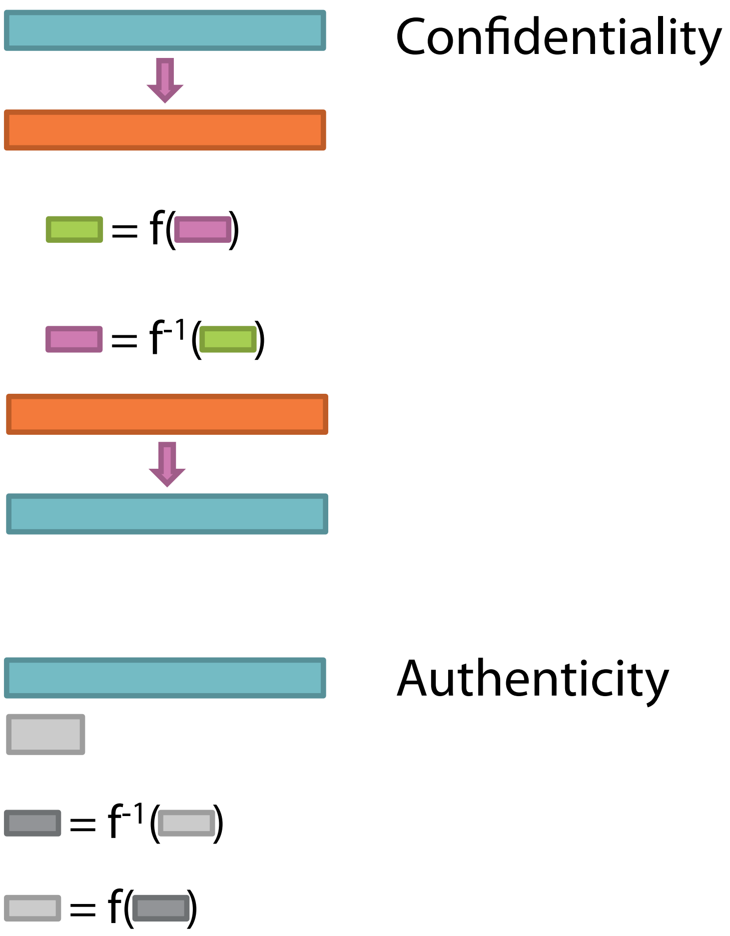
Never sign someone else's document

Always append randomness

Identity

Private key – $f^{-1}(x)$

Public key – $f(x)$

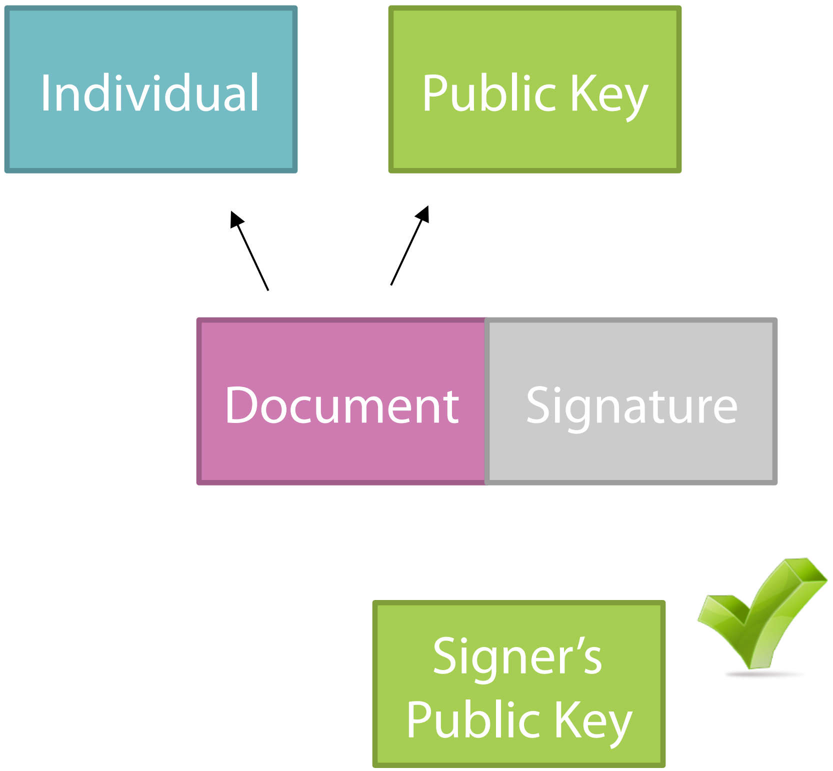


Trust ?

Trust

- **Direct key exchange**
- **Community**
  - Do others trust this key?
  - Web of trust
  - Have to trick many people
  - PGP
- **Authorities**
  - Vouch for identity
  - Chain of trust
  - X.509 certificates

Sign Public Keys



Summary

- **Asymmetric**
  - RSA
  - Elliptic Curve
- **Symmetric**
  - DES
  - AES
- **Hash Functions**
  - MD5
  - SHA 1, 2, and 3
- **Confidentiality**
  - Encrypt message with symmetric
  - Encrypt key with public
- **Authenticity**
  - Compute digest with hash
  - Encrypt digest with private