Making and Breaking Ciphers

Ralph Morelli

Trinity College, Hartford

(ralph.morelli@trincoll.edu)

Smithsonian Institute
October 31, 2009

Trinity College
HARTFORD CONNECTICUT

This presentation was created using Open Office 3.0,
free and open source software.
http://www.openoffice.org/

Part III: Computerized Cryptology

Outline

- Vernam Cipher – perfect secrecy
- Computerization: From Letters to Bits
- DES
- The Key Exchange Problem
- Public Key Cryptography
- Quantum Cryptography

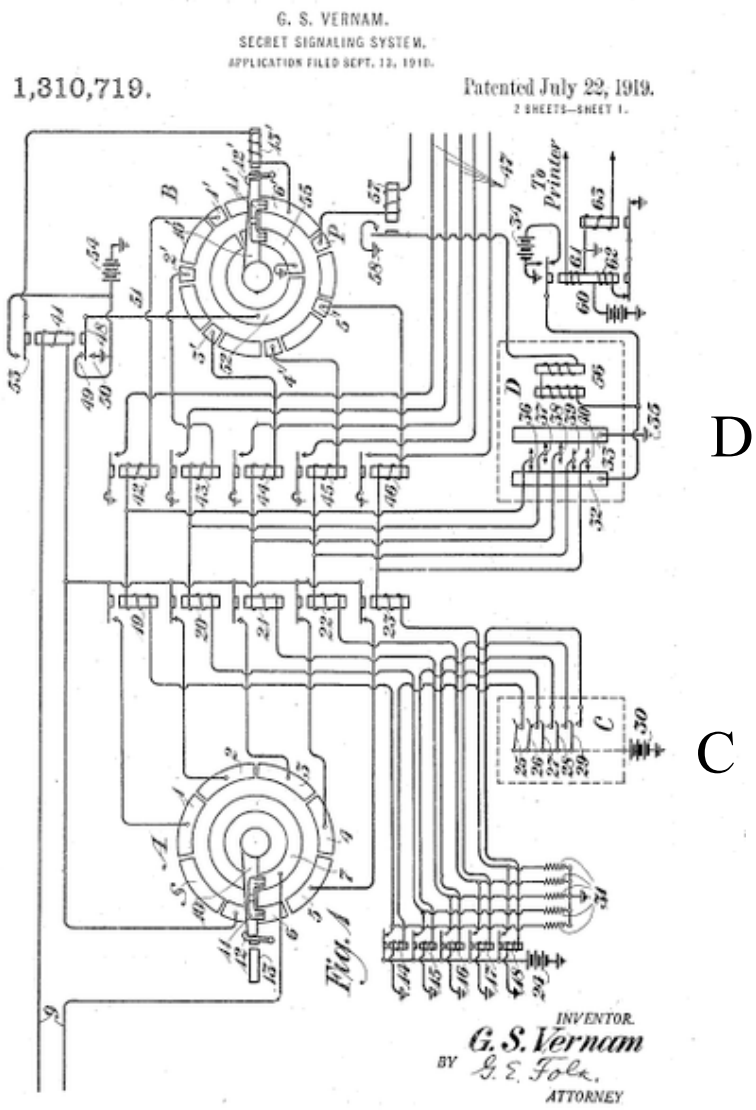
Perfect Secrecy

Vernam Cipher

- Gilbert S. Vernam, AT&T, 1919
- Morse code – 5 pulses per character.
- A = (mark mark space space space)
- Vernam's: Add a key tape to the message:

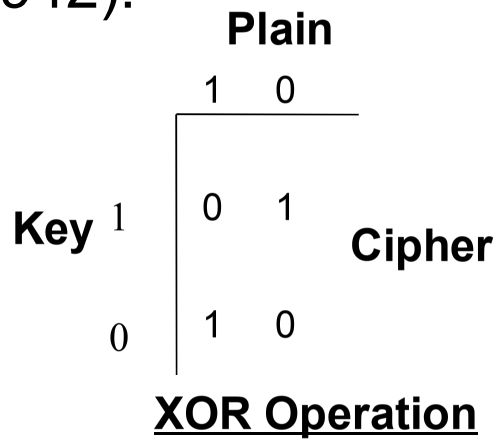
Plaintext	Key	Ciphertext
mark	mark	space
mark	space	mark
space	mark	mark
space	space	space

- Reversible, one-step encryption and decryption using a key loop tape.
- Flaw: repeating key is polyalphabetic.



One Time Pad

- Generalization of Vernam: make the key as long as the message.
- Provably perfect secrecy (Claude Shannon, 1942):
  - Secret key.
  - Of truly random characters.
  - As long as the message.
  - Used only once and then discarded.
- Example:



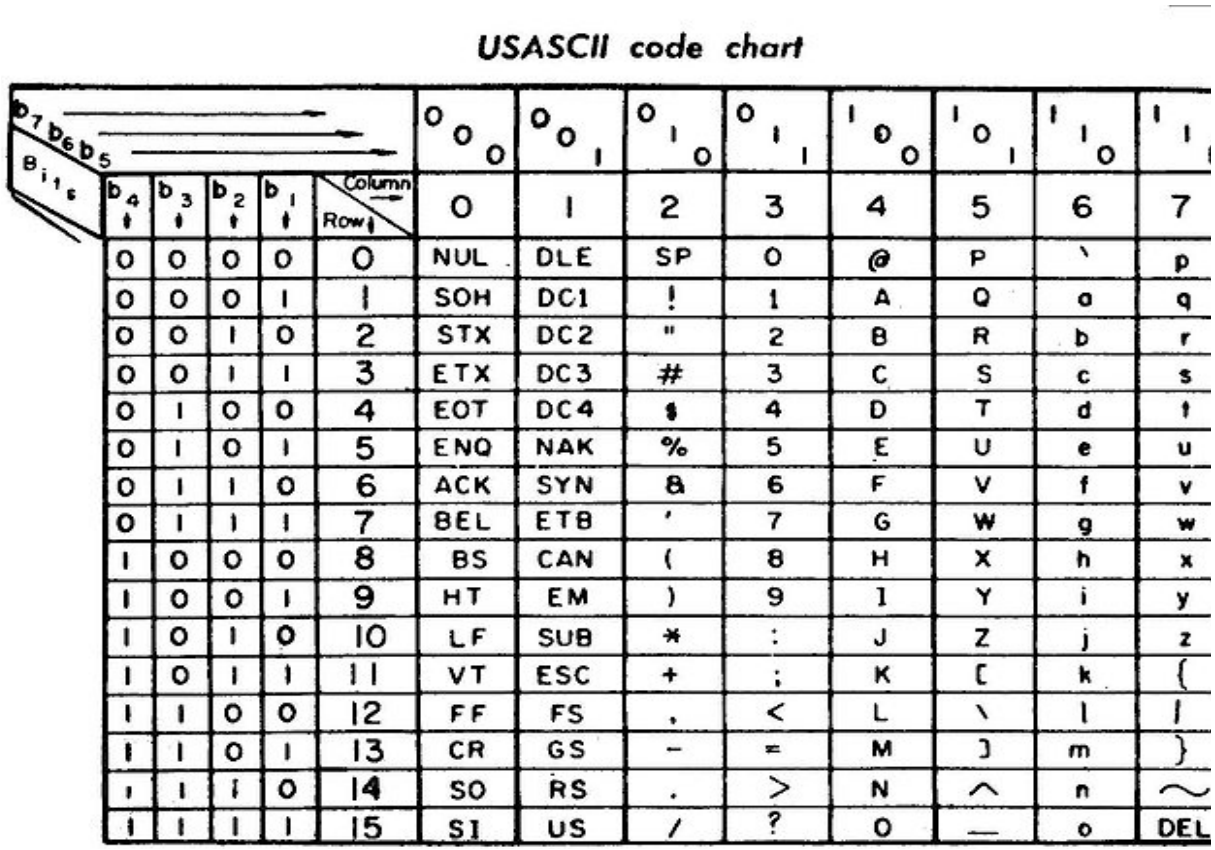
	Plaintext:	01101 10101 01111 10110 10101
Encrypt	Key:	01010 10100 11101 01011 10110
	Ciphertext:	00111 00001 10010 11101 00011
	Key:	01010 10100 11101 01011 10110
Decrypt	Plaintext:	01101 10101 01111 10110 10101

Theoretical Principles

- Claude Shannon, 1949, “Communication Theory of Secrecy Systems,” Bell Labs.
- Perfect secrecy property.
- Confusion – maximum complexity between the key and ciphertext.
- Diffusion – plaintext uniformities (statistics) are dissipated in the ciphertext.
- A cipher system should be secure even if its algorithm is known (Kerchoff's principle).

ASCII Code

- Developed from telegraph codes.
- 1963 Standard
- 1966 chart
- A=100 0001
- B=100 0010
- C=100 0011



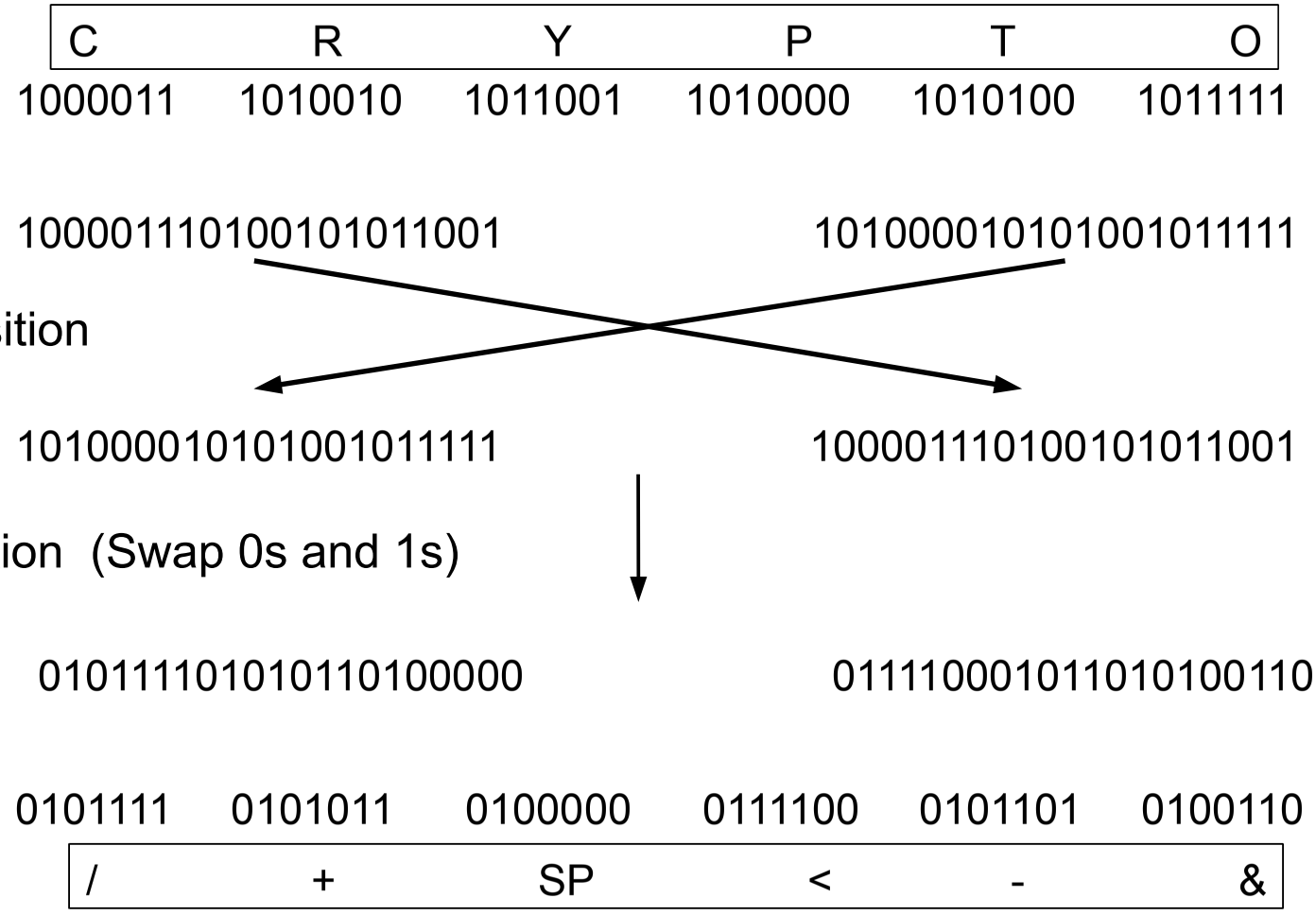
USASCII code chart

Bits b_4 b_3 b_2 b_1	Row	Col 0 (000)	Col 1 (001)	Col 2 (010)	Col 3 (011)	Col 4 (100)	Col 5 (101)	Col 6 (110)	Col 7 (111)
0 0 0 0	0	NUL	DLE	SP	0	@	P	`	p
0 0 0 1	1	SOH	DC1	!	1	A	Q	a	q
0 0 1 0	2	STX	DC2	"	2	B	R	b	r
0 0 1 1	3	ETX	DC3	#	3	C	S	c	s
0 1 0 0	4	EOT	DC4	$	4	D	T	d	t
0 1 0 1	5	ENQ	NAK	%	5	E	U	e	u
0 1 1 0	6	ACK	SYN	&	6	F	V	f	v
0 1 1 1	7	BEL	ETB	'	7	G	W	g	w
1 0 0 0	8	BS	CAN	(	8	H	X	h	x
1 0 0 1	9	HT	EM	)	9	I	Y	i	y
1 0 1 0	10	LF	SUB	*	:	J	Z	j	z
1 0 1 1	11	VT	ESC	+	;	K	[	k	{
1 1 0 0	12	FF	FS	,	<	L	\	l	|
1 1 0 1	13	CR	GS	-	=	M	]	m	}
1 1 1 0	14	SO	RS	.	>	N	^	n	~
1 1 1 1	15	SI	US	/	?	O	_	o	DEL

1000011 1010010 1011001 1010000 1010100 1011111

C R Y P T O

Transposition and Substitution



- Transposition
- Substitution (Swap 0s and 1s)

XOR: Substitution with a Key

- Plain Message

C	R	Y	P	T	O

- ASCII: 1000011 1010010 1011001 1010000 1010100 1011111
- KEY= ABCDEF: 1000001 1000010 1000011 1000100 1000101 1000110

- msg XOR key: 0000010 0010000 0011010 0010100 0010001 0011001

A	B	A ⊕ B
0	0	0
0	1	1
1	0	1
1	1	0

- Crypto Message: 0000010 0010000 0011010 0010100 0010001 0011001
- KEY= ABCDEF: 1000001 1000010 1000011 1000100 1000101 1000110

- Plain Message: 1000011 1010010 1011001 1010000 1010100 1011111

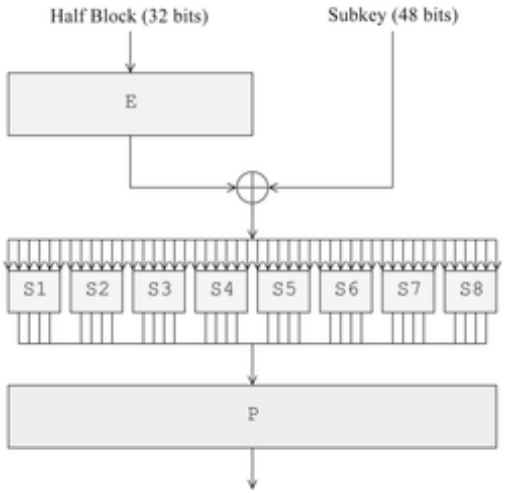
C	R	Y	P	T	O

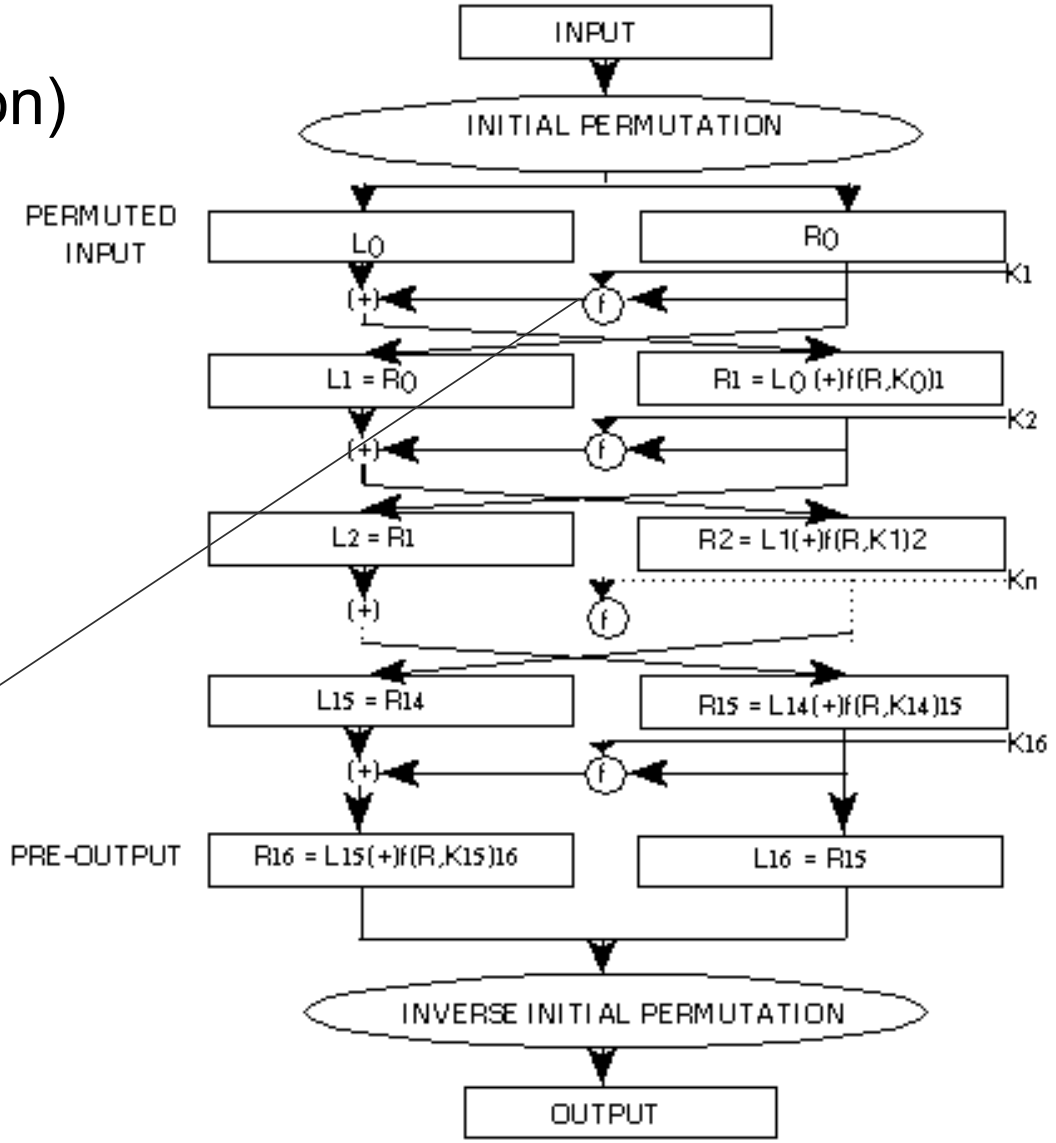
Data Encryption Standard (DES)

- Early 1970s: IBM and NSA Collaboration.
- 1976: Adopted as the federal IP standard.
- Controversial among cryptographers.
  - Key too short.
  - Classified elements in the algorithm.
  - NSA backdoor?
- 1999: EFF broke it in 23 hours (brute force).
- 2002: Replaced after public competition by Advanced Encryption Standard (AES)

DES Algorithm
(Trasposition & Substitution)

- 64-bit block cipher
- 56-bit key (+ 8 bits parity)
- Feistel mixing: 16 cycles of transposing and XORing with 48-bit subkeys (K_1...K_{16})

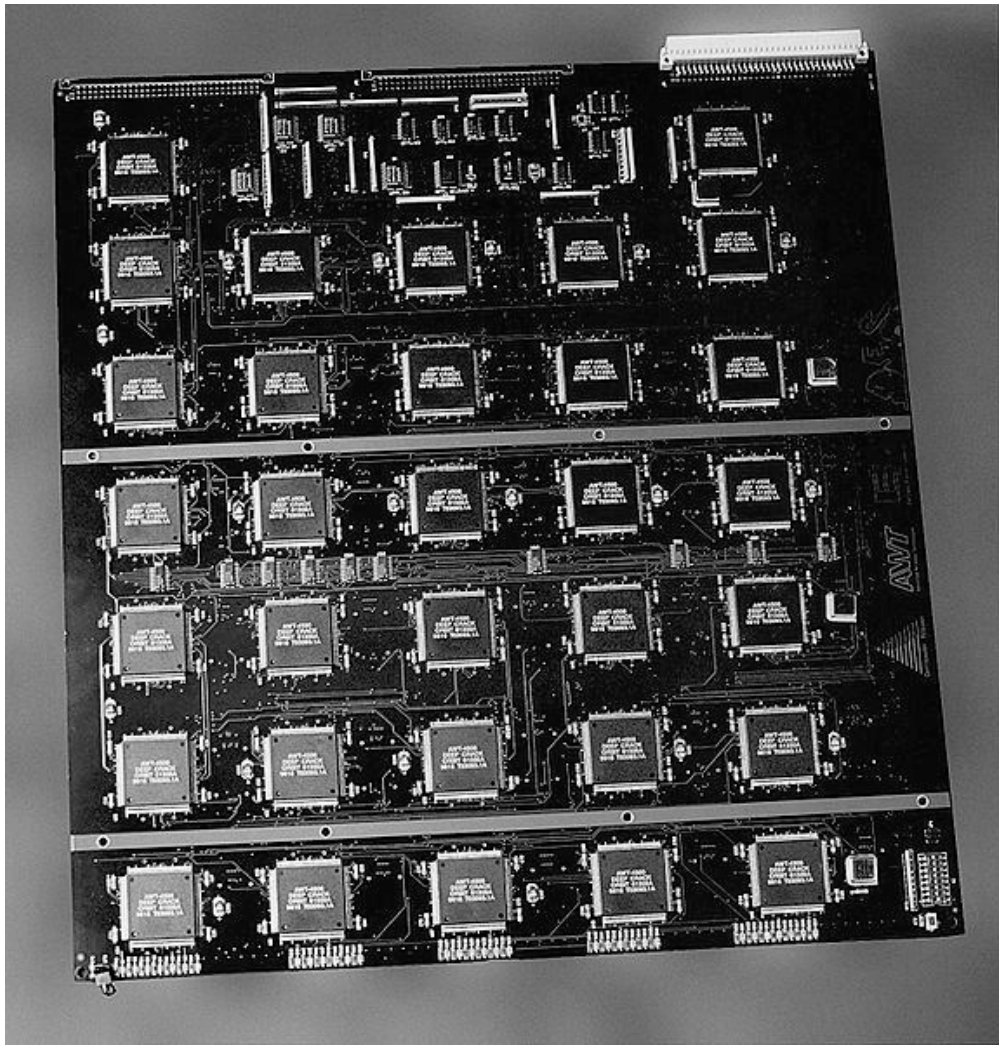




Source: FIPS PUB 46-2http://www.itl.nist.gov/fipspubs/fip46-2.htm

EFF's DES Deep Crack

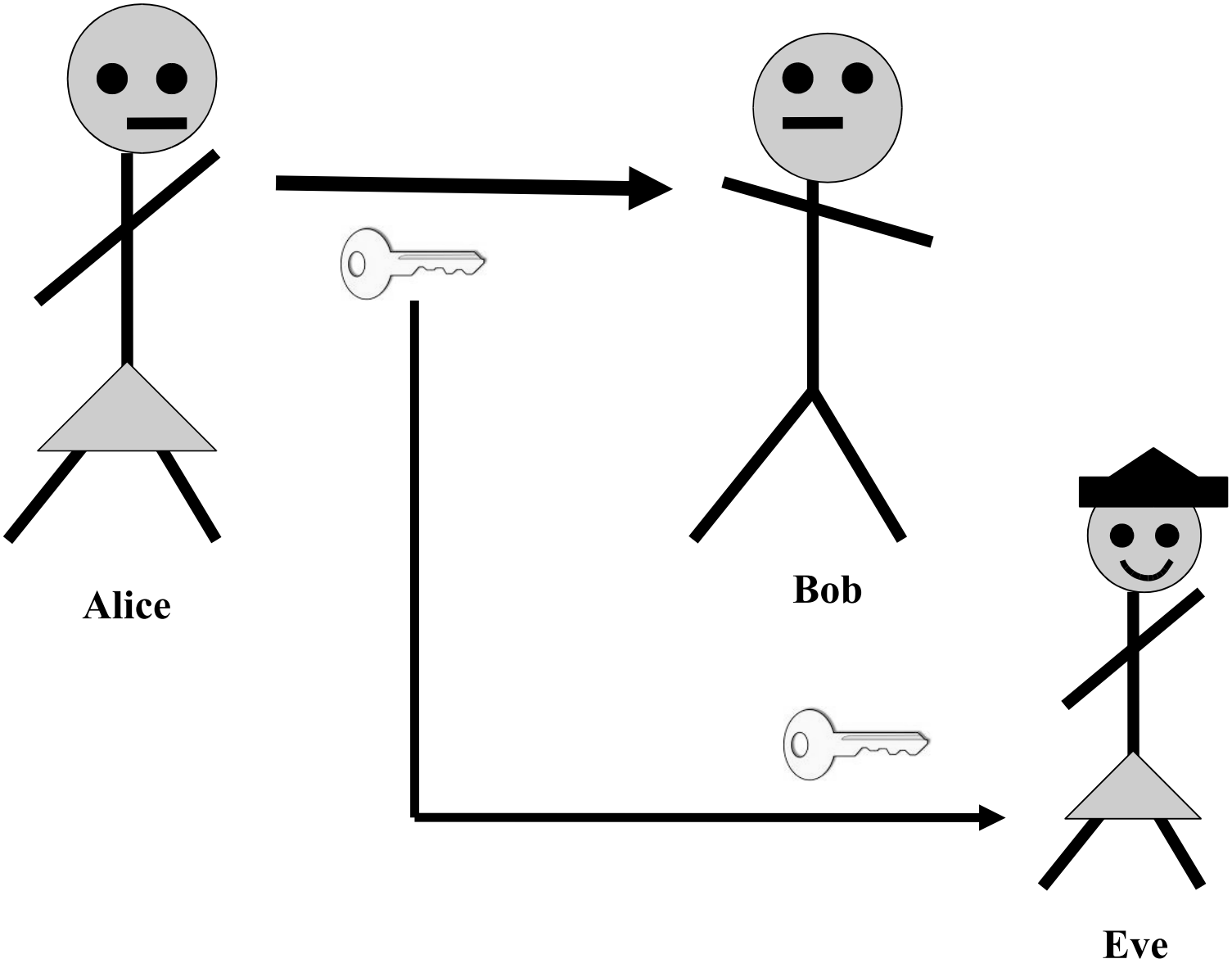
- Specialized chips
- $250,000
- 1998 – 56 hours.
- 1999 – 22.25 hrs. with distributed.net.
- 1999: DES reaffirmed as the standard with Triple-DES recommended.



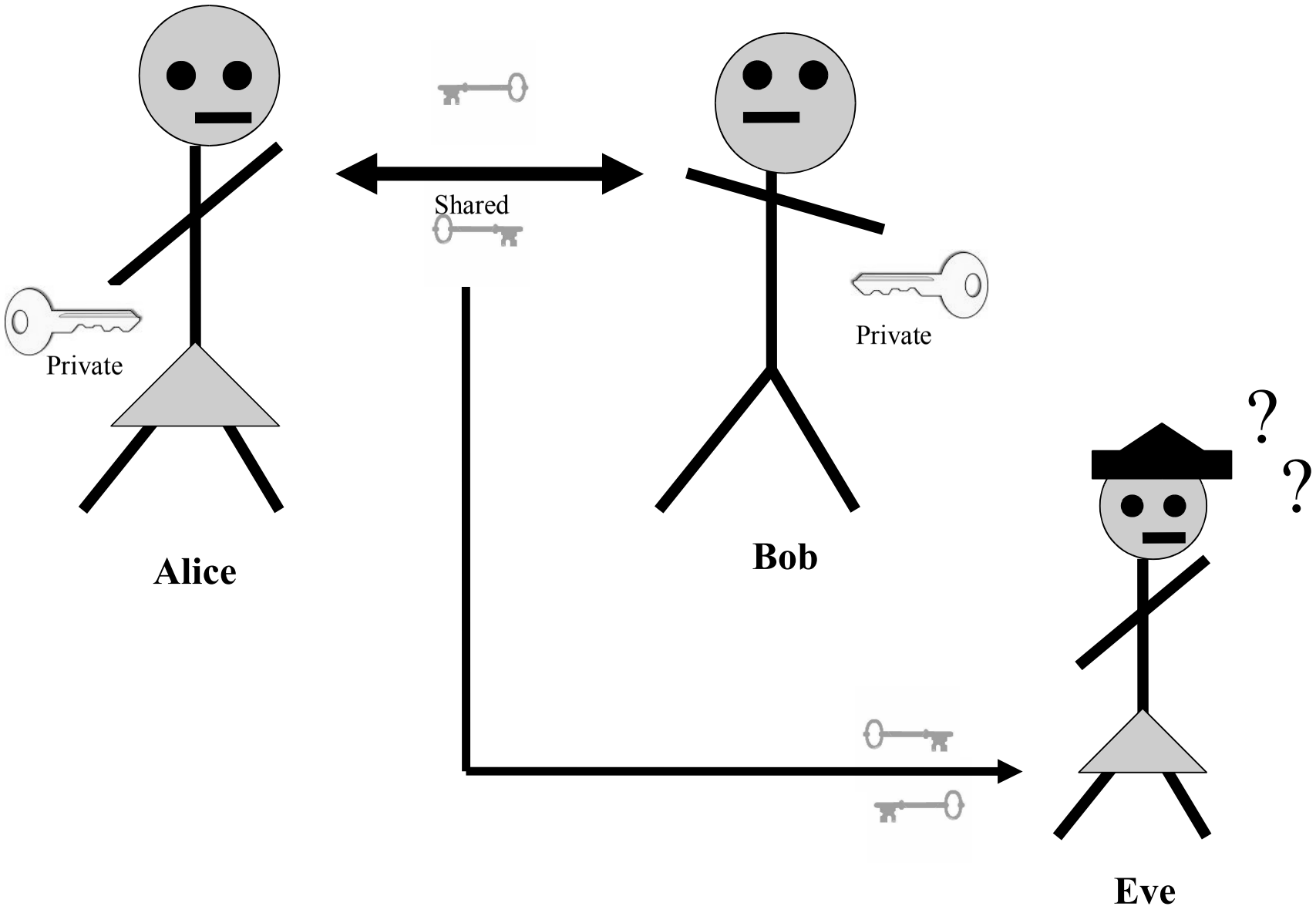
Symmetric vs. Asymmetric Keys

- Symmetric Key
  - Same key used for encryption and decryption.
  - Must be shared by Alice and Bob.
  - Key exchange problem.
- Asymmetric Key –
  - Different keys used for encryption and decryption.
  - No key exchange problem.

The Key Exchange Problem



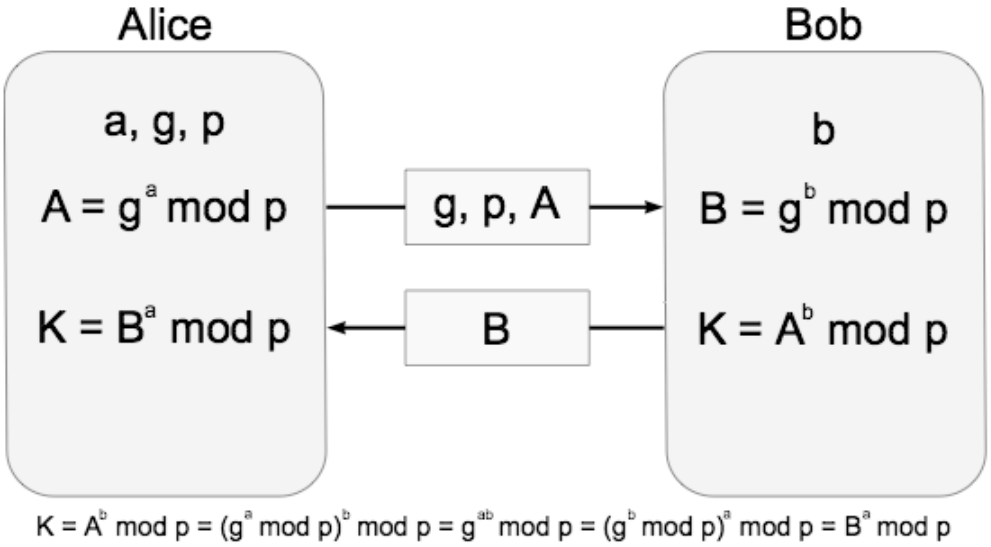
Asymmetric Keys



Diffie-Hellman Key Exchange

- Invented in 1976
- Modular arithmetic: (8 + 7) mod 12 = 3
  - 8 AM + 7 hours = 3 PM
  - 8 + 7 = 15 mod 12 = 1 Rmdr = 3
  - (8 * 7) mod 12 = 56 mod 12 = 4 Rmdr = 8
- One-way function
  - $3^x = 1 \pmod 4$ What is x? {2, 4, 6, … }

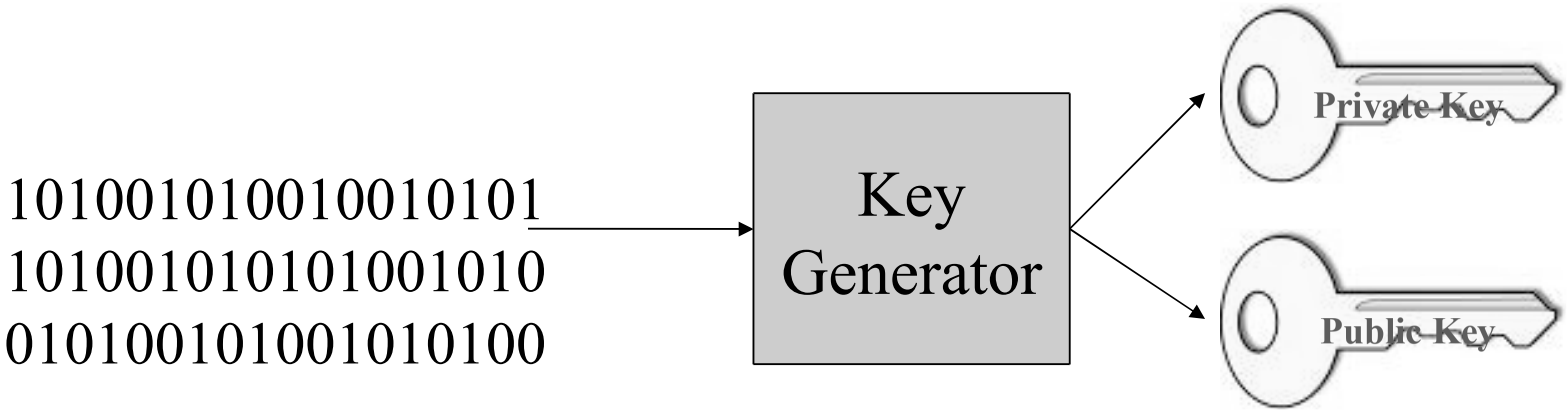
Diffie-Hellman Key Exchange



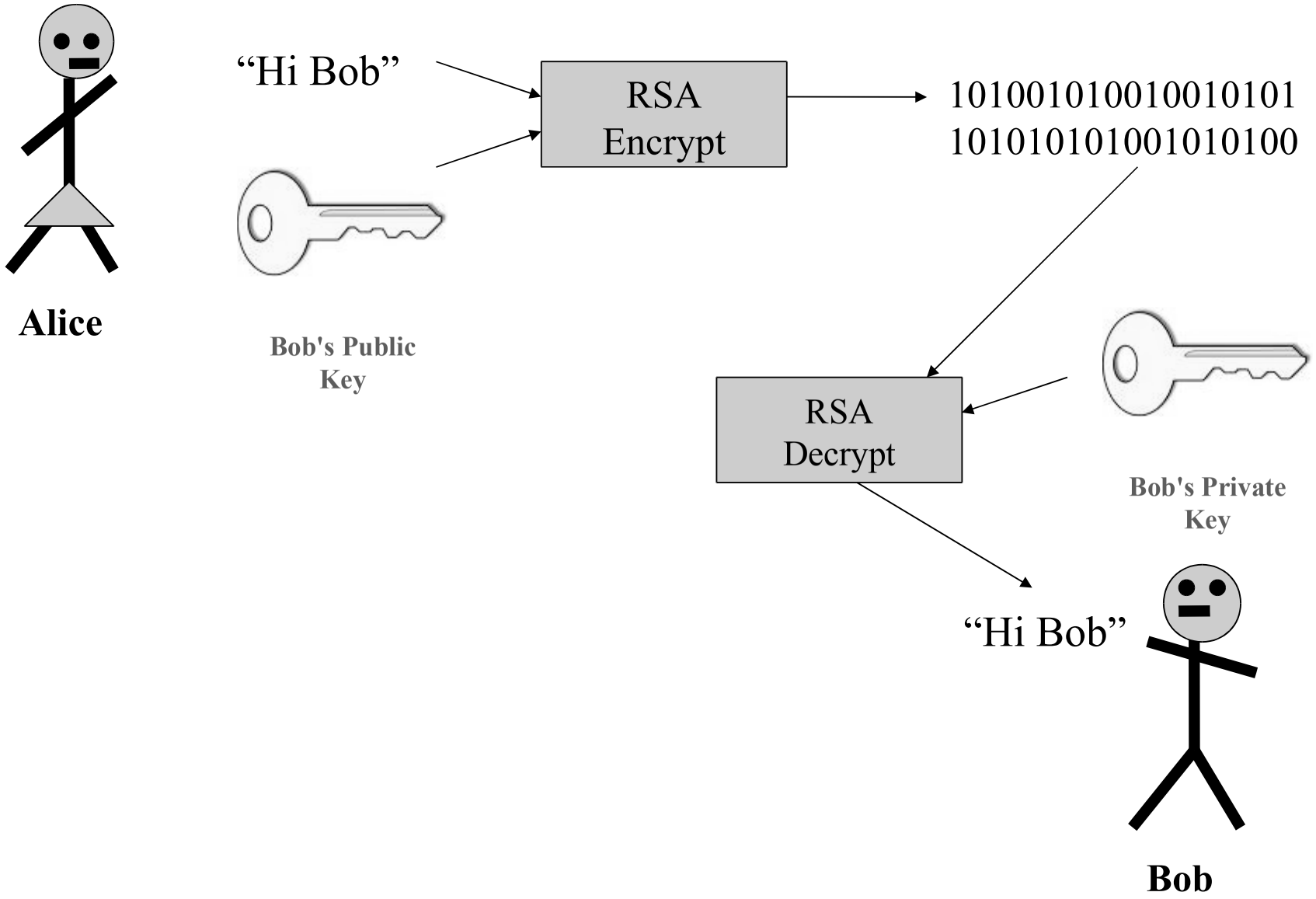
- Alice's secret number is *a* and Bob's secret number is *b*.
- They agree on the base *g* and prime number *p* and the function $g^x \ (mod\ p)$.
- They exchange $A = g^a \ (mod\ p)$ and $B = g^b \ (mod\ p)$.
- They derive the same key *K* because $g^{ab} (mod\ p) = g^{ba} (mod\ p)$.
- Eve can't easily derive *K* without knowing *a* and *b*.

Public Key Cryptography

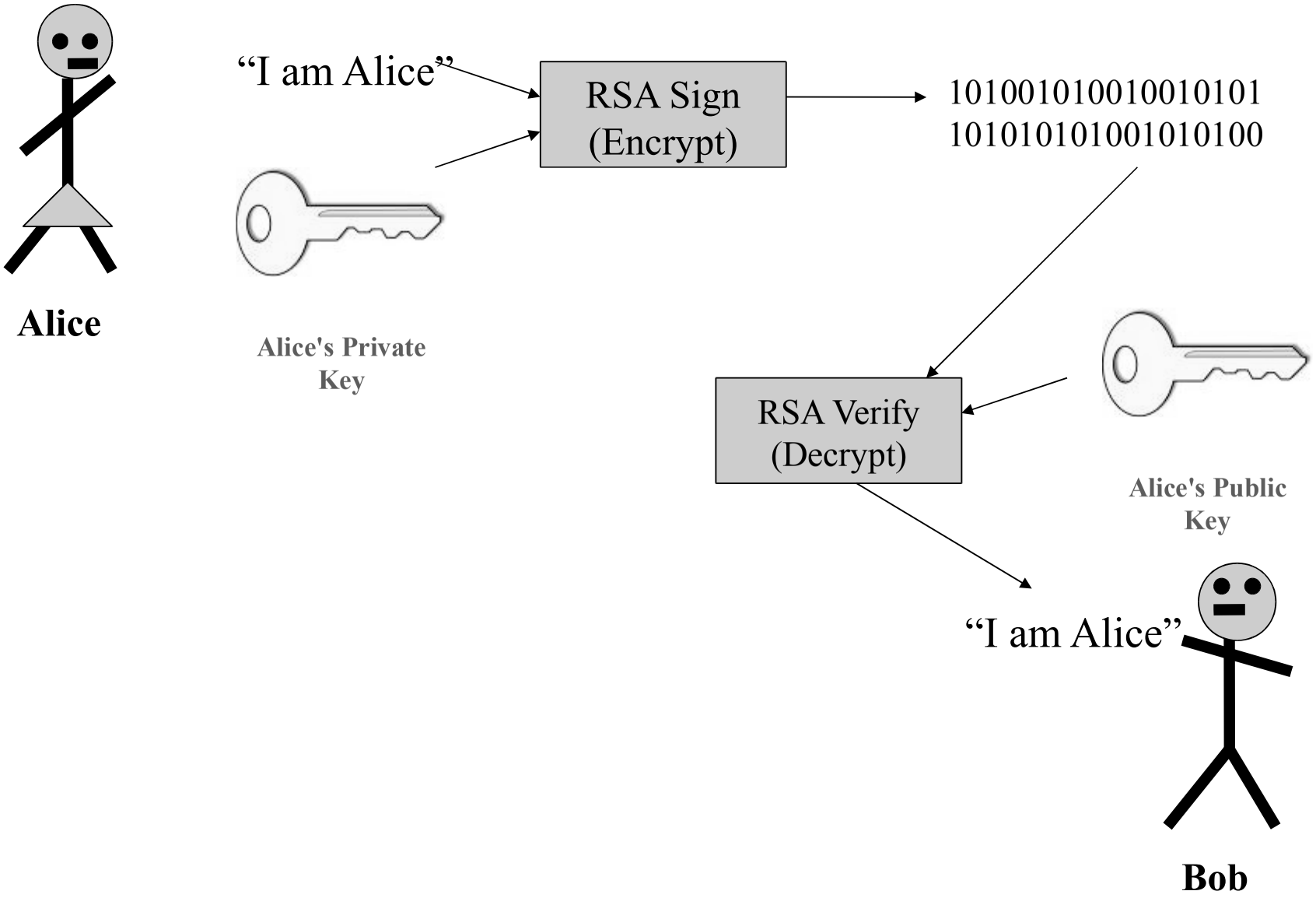
- 1984 Rivest-Shamir-Adelman Algorithm (RSA)
- Based on the difficulty of computing prime factors.
- Asymmetric key (public/private part) vs. symmetric key (shared by Alice and Bob)



Public Key Encryption/Decryption



Public Key Signature



RSA Details

- Alice picks two huge prime numbers, *p* and *q.*
- Alice computes *N = p x q.*
- Alice picks another number *e* relatively prime to (p-1) x (q-1).
- Alice calculates her private key *d* as:

  d x e = 1 (mod (p-1) * (q-1))
- Alice publishes (N, e) as her public key.
- Encrypt message to Alice, *M:* $C = M^e \pmod N$
- Alice decrypts message, *C:* $M = C^d \pmod N$

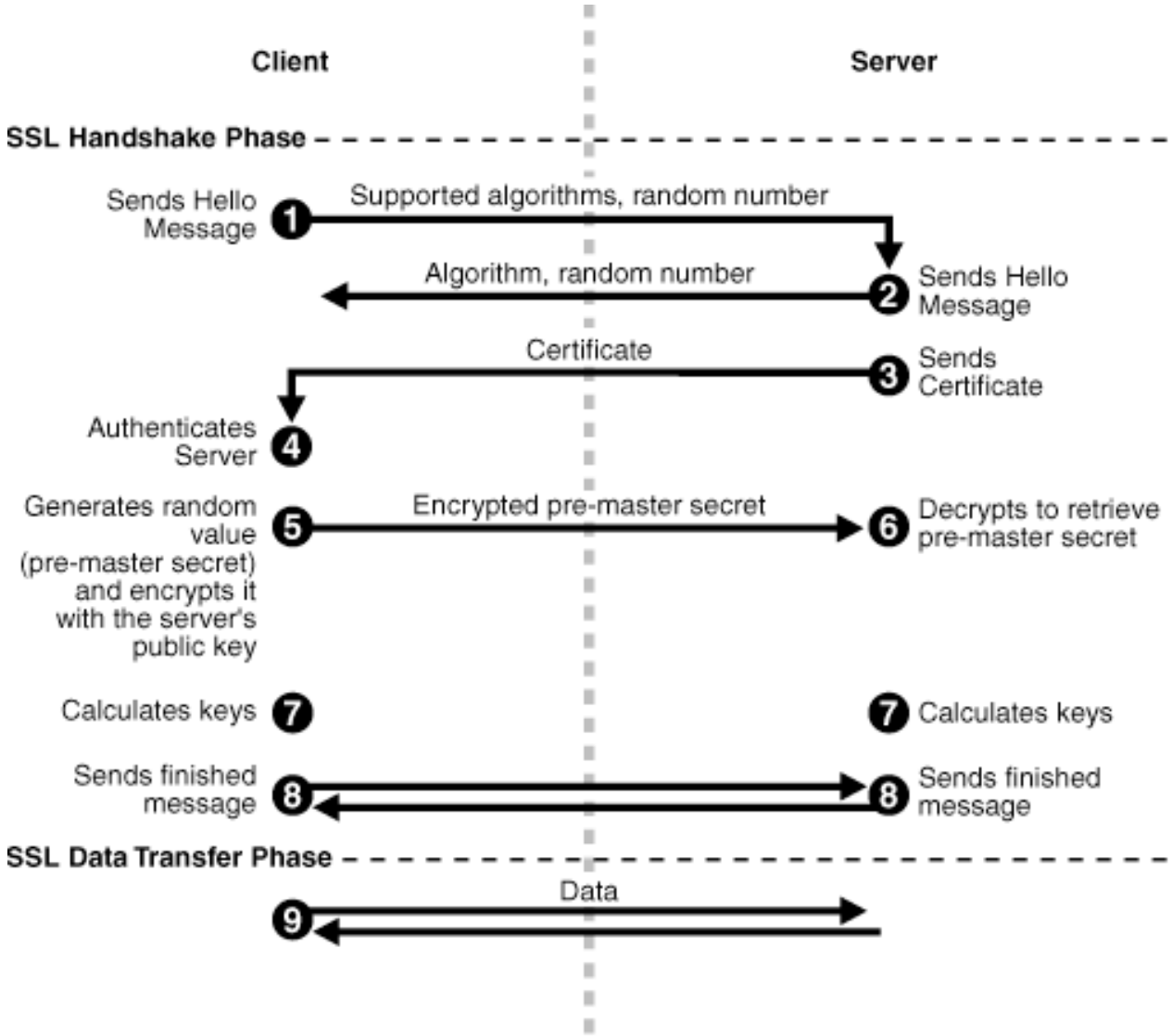
RSA Security

- Given $N = p \times q$, why can't we just figure out the primes p and q?
- Factorization of N: For each prime number, n_i check if it divides N.
- How big is N? ~ 10^{308} for bank transactions.
- Best estimate: 100 million computers working together would take more than 1000 years (Simson Garfinkel, as reported in Singh).

Internet Security

- Transport Layer Security (Secure Sockey Layer)
- Client (user's browser) and server (e.g., user's bank) communication protocol.
- Phase 1: Client and server negotiate which algorithms will be used for key exchange and authentication (typically public key algorithms).
- Phase 2: A symmetric key is exchanged and authenticated.
- Phase 3: Encrypted, efficient communication using the symmetric key.

Transport Layer Security



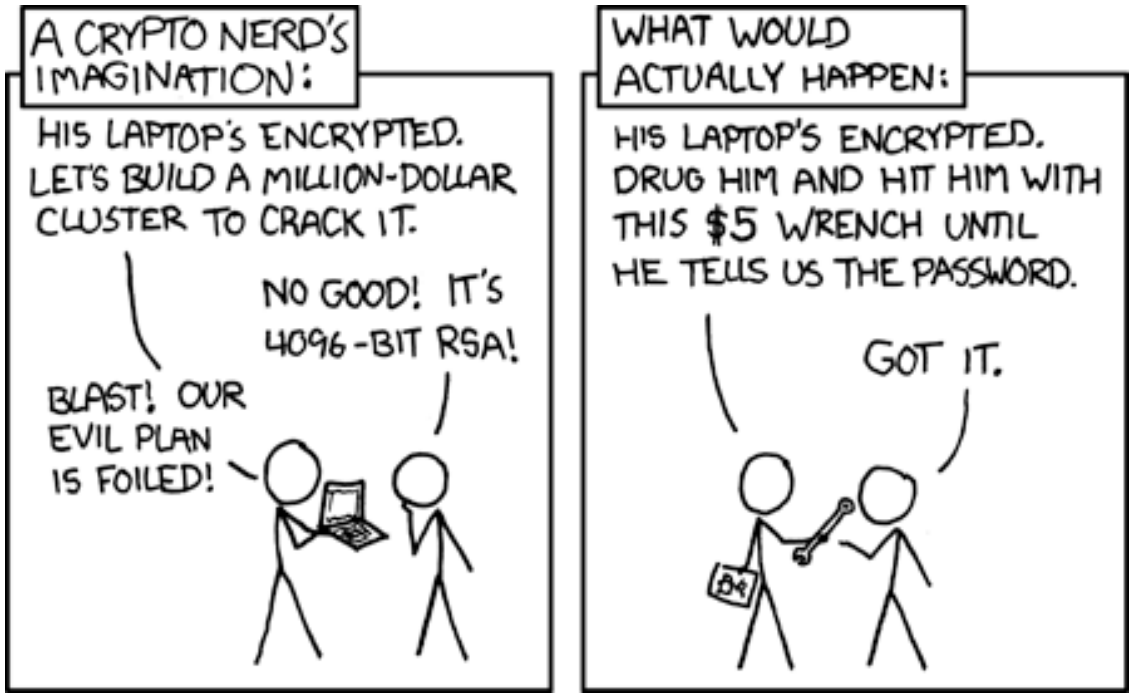
Quantum computation: A quantum computer could easily break a factorization problem.

Quantum Cryptography

Alice's random bit	0	1	1	0	1	0	0	1
Alice's random sending basis	+	+	×	+	×	×	×	+
Photon polarization Alice sends	↑	→	↘	↑	↘	↗	↗	→
Bob's random measuring basis	+	×	×	×	+	×	+	+
Photon polarization Bob measures	↑	↗	↘	↗	→	↗	→	→
PUBLIC DISCUSSION OF BASIS								
Shared secret key	0		1			0		1

- BB84 Protocol: Charles H. Bennet and Gilles Brassard, 1984. (IBM, University of Montreal)
- Exchange random bit stream for use in one-time pad.
- Possible to detect an eavesdropper.
- Implementations: Exchange secure keys over optical fiber at 1 Mbit/s (10 km) and 10 kbits/s 100 km.
- Much research (IBM, NEC, HP, Toshiba, Mitsubishi)
- Four commercial companies

Perfect Secrecy!?



Source: http://xkcd.com/