Introduction to Public-Key Technology

Burt Kaliski
RSA Laboratories

1993 RSA Data Security Conference

Outline

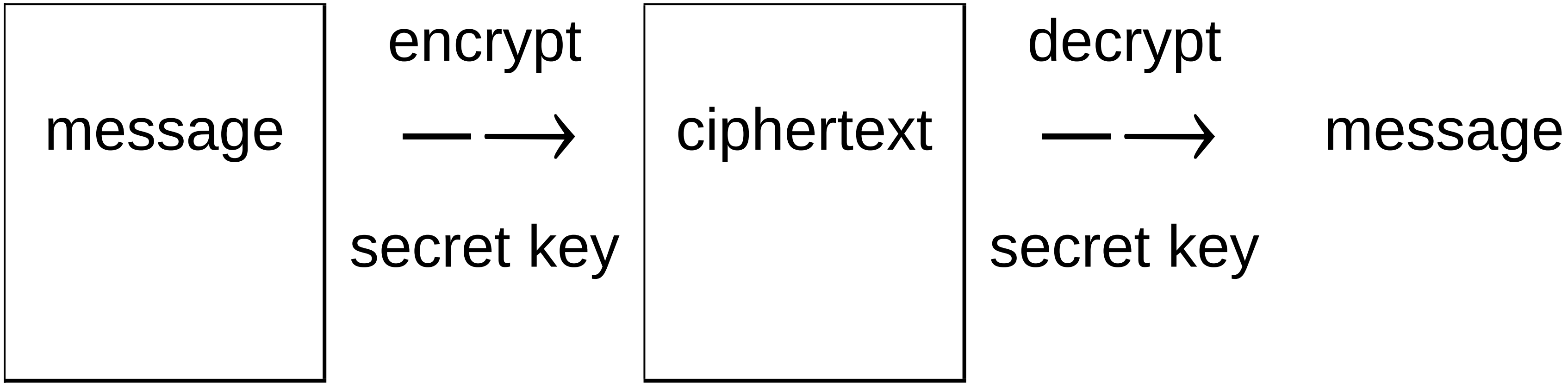
- **Concepts**
  - Secret key, public key, message digest, ...
- **Algorithms**
  - DES, RSA, DSS, ...
- **RSA Details**
- **Applications**
  - Digital signatures and envelopes
- **Standards**
- **Conclusions**

Concepts

Secret-key cryptosystem

Encryption, decryption with same key.

For privacy.



message

encrypt

secret key

ciphertext

decrypt

secret key

message

Users agree secretly on key.

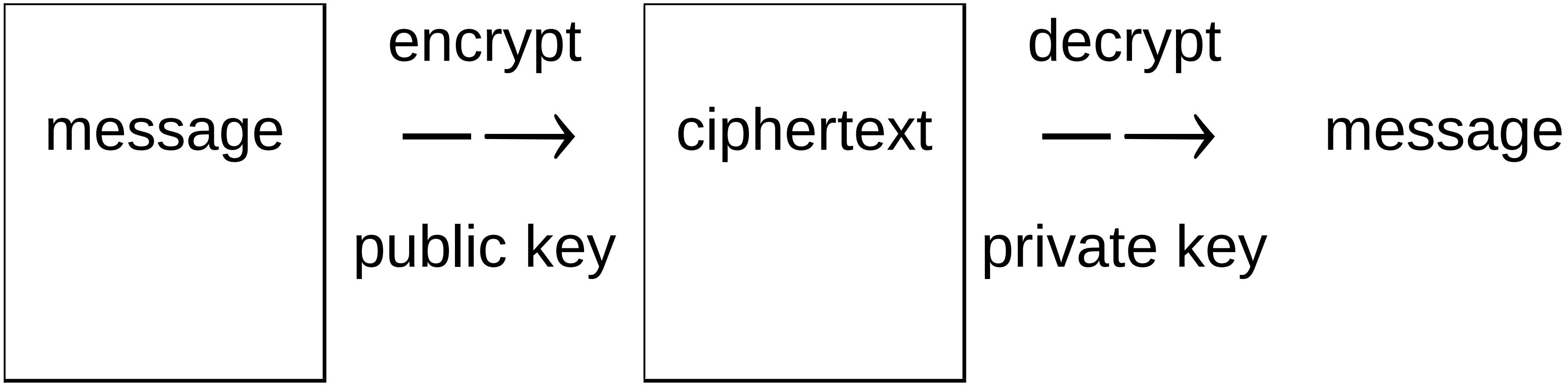
Examples: DES, RC2, RC4.

Concepts (cont'd)

Public-key cryptosystem

Encryption, decryption with different keys.

For privacy.



message

encrypt → public key

ciphertext

decrypt → private key

message

Users keep one key private, publish other.

Examples: RSA, ElGamal.

Often hybrid with secret key.

Concepts (cont'd)

Secret key vs. public key

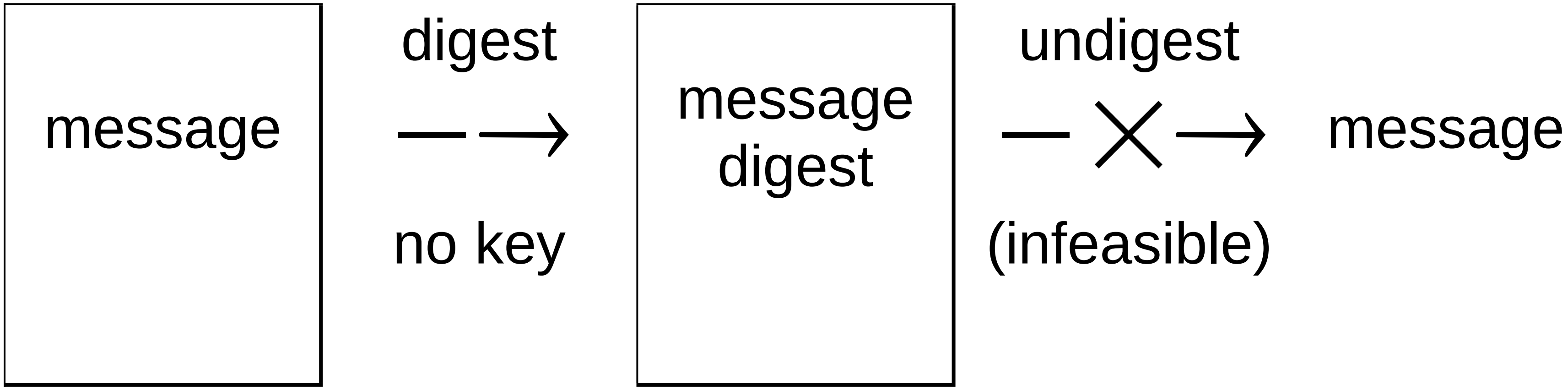
	secret key	**public key**
copies/ secret	two	one
secrets/user	many	one
scalability	fair	good
speed	good	fair

Hybrid cryptography combines benefits.

Concepts (cont'd)

Message-digest algorithm

For "fingerprinting"—one-way hash.



message

digest

no key

message digest

undigest

(infeasible)

message

Typically 128 or 160 bits.

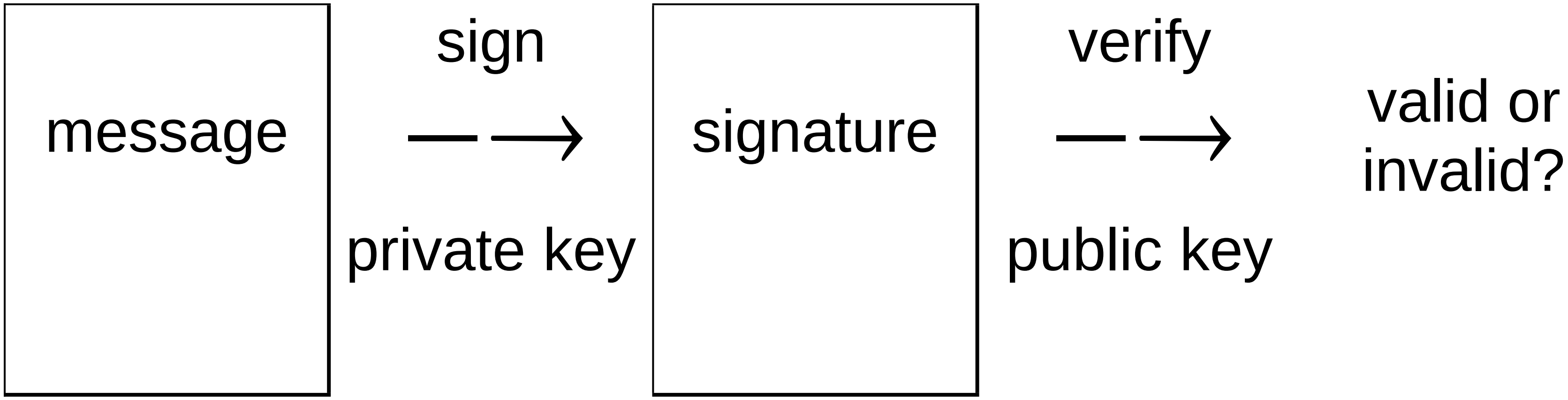
Examples: MD5, SHS.

Concepts (cont'd)

Digital signature scheme

Signature with private key, verification with public.

For authentication—of message and signer.



message

sign

private key

signature

verify

public key

valid or invalid?

Examples: RSA, DSS.

Usually hybrid with message digest.

Algorithms

Data Encryption Standard (DES)

NBS, 1976

Secret-key cryptosystem

56-bit keys

RSA

Rivest-Shamir-Adleman, MIT, 1977

Public-key cryptosystem *and* digital signature scheme

Based on difficulty of factoring large integers

Algorithms (cont'd)

RC2, RC4

Rivest, RSADSI, 1980s

Block & high-speed stream secret-key cryptosystems

Variable-length keys

MD5

Rivest, MIT/RSADSI, 1991

High-speed message-digest algorithm

128-bit digest

Algorithms (cont'd)

Digital Signature Standard (DSS)

- NIST, 1991
- Digital signature scheme
- Based on difficulty of discrete logarithms

Secure Hash Standard (SHS)

- NIST, 1992
- High-speed, DSS-compatible message-digest algorithm
- 160-bit digest

RSA Details

Keys

n: public modulus

e: public exponent (typically 3 or $2^{16}+1$)

d: private exponent

p,*q*: private factors of modulus

$$n = p \times q$$

$$d \times e \text{ mod } (p\text{-}1)(q\text{-}1) = 1$$

Public key is (*n*,*e*).

Private key is (*n*,*d*).

RSA Details (cont'd)

Encryption with public key

m: message

Ciphertext = c where

$$c = m^e \bmod n.$$

m may be a key.

Decryption with private key

$$m = c^d \bmod n.$$

RSA Details (cont'd)

Encryption with private key

Signature = s where

$$s = m^d \bmod n.$$

m may be a message digest.

Decryption with public key

$$m = s^e \bmod n.$$

RSA Details (cont'd)

Performance

RSA operations involve *modular multiplication*, which takes time proportional to (log *n*)^2.

Public-key: 2 to 17 multiplications

Private-key: 1.5 log *n* multiplications

Given *p*, *q*, four times faster.

Good public-key speed, fair private-key speed —but good in combination with secret key, message digest.

RSA Details (cont'd)

Performance (cont'd)

Examples with 512-bit keys, $e = 2^{16}+1$, given p, q:

Processor	Public key (sec.)	Private key (sec.)
16 MHz 68020	.32	3.3
12 MHz 80286	.25	2.7
25 MHz 68040	.065	.65
20 MHz 80386	.065	.55

30 MHz DSP16A	.035	.17
20MHz DSP56000	.0081	.044

For 1024 bits, public key × 4, private key × 8.

RSA Details (cont'd)

Security

Goal: Given n, find p and q.

Typical approaches take time

$$L(n) = \exp((1+\varepsilon)).$$

$L(n)$ is *subexponential* in $\log_2 n$:

For any constant c, $L(n)$ grows slower than n^c (exponential), faster than $(\log_2 n)^c$ (polynomial).

Thus, hardware speedups help multiplication more than factoring.

RSA Details (cont'd)

Security (cont'd)

Based on $L(p)$ as instruction count (Rivest, 1991):

$\log_2 n$	$L(n)$	MIPS years
512	6.7×10^{19}	2.1×10^{6}
576	1.7×10^{21}	5.5×10^{7}
	· · ·	
960	3.7×10^{28}	1.2×10^{15}

1024	4.4×10^{29}	1.4×10^{16}

MIPS year = one million instructions/second for one year = 3.1×10^{13} intructions.

$2^{56} \approx 7.2\times10^{16}$ (not directly comparable).

Applications

Hybrid cryptography

Digest + public key = digital signature.

Secret key + public key = digital envelope.

Performance, scalability, no shared secrets.

Two tools

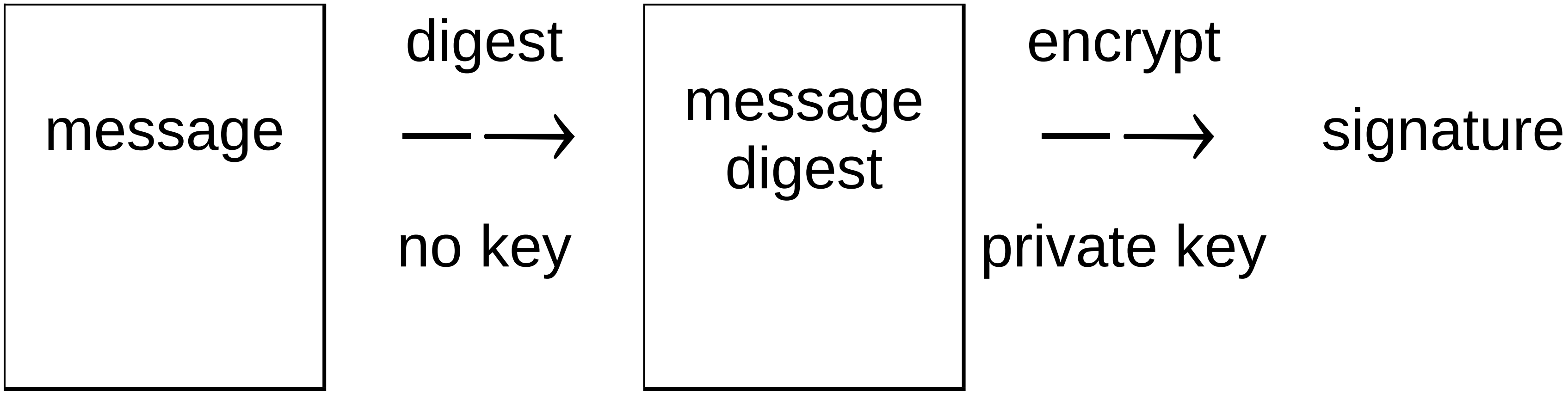
Digital signatures: *sign* and *verify*.

Digital envelopes: *seal* and *open*.

Applications (cont'd)

Signing a message

Alice digests message, encrypts signature with her private key.



message

digest

$\longrightarrow$

no key

message digest

encrypt

$\longrightarrow$

private key

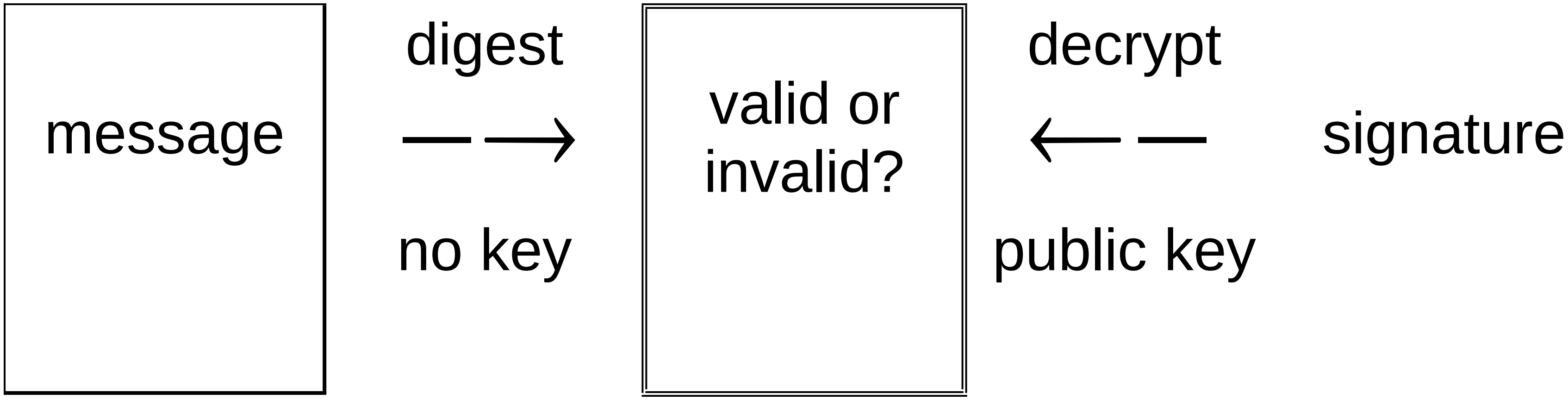
signature

She sends the message and signature to Bob.

Applications (cont'd)

Verifying a signature

Bob digests message, decrypts signature with Alice's public key, compares results.



message

digest

no key

valid or invalid?

decrypt

public key

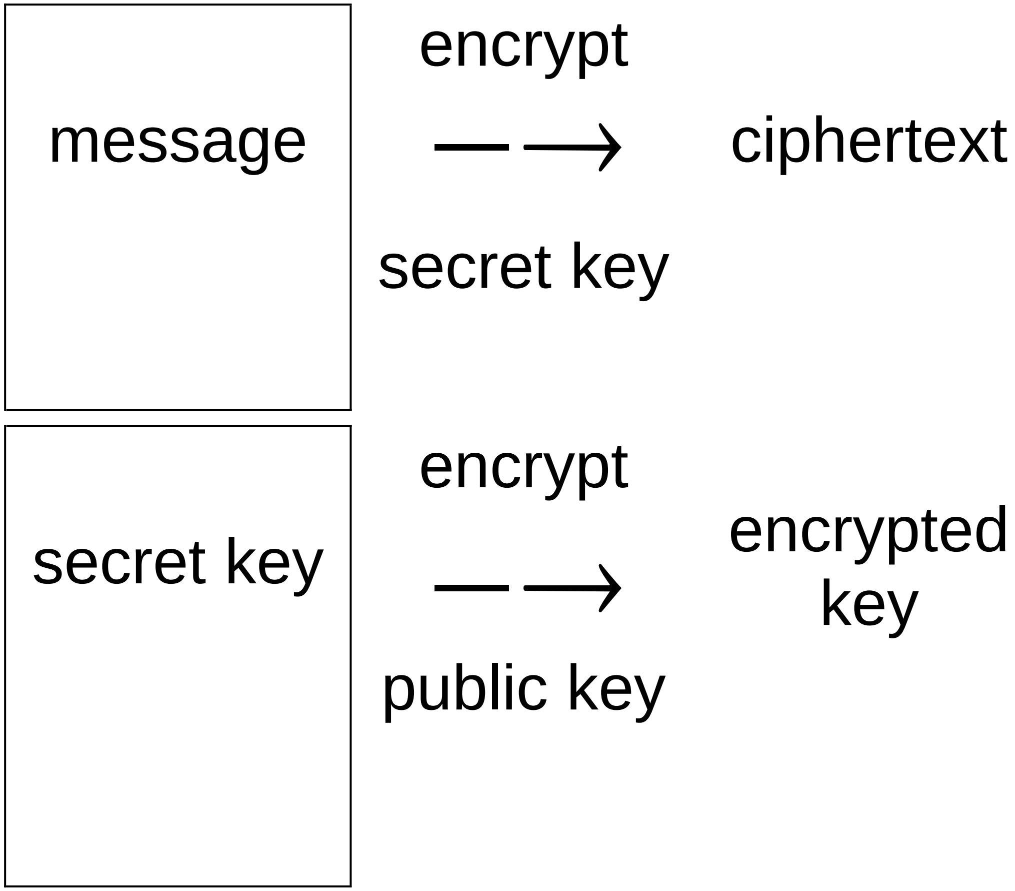
signature

The signature is valid if and only if the results are the same.

Applications (cont'd)

Sealing a message

Alice encrypts message with a secret key,
encrypts secret key with Bob's public key.



message

encrypt

secret key

ciphertext

secret key

encrypt

public key

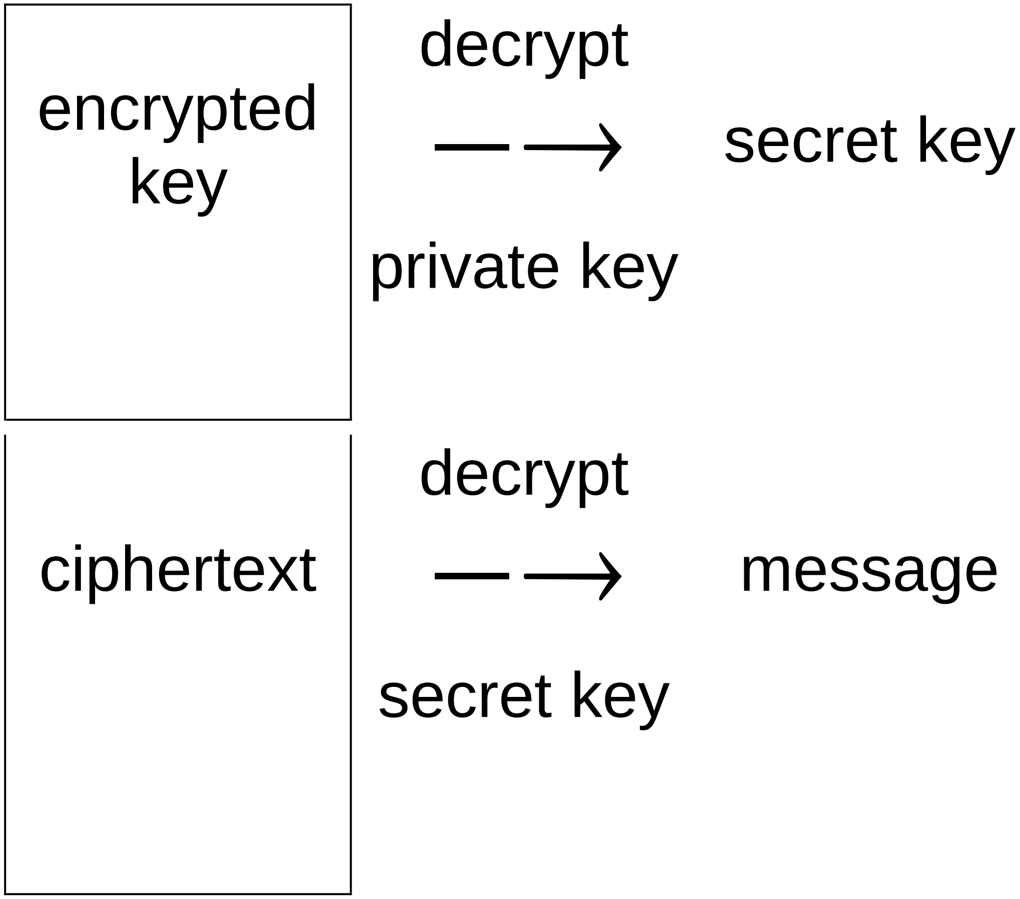
encrypted key

She sends the ciphertext and encrypted key to Bob.

Applications (cont'd)

Opening an envelope

Bob decrypts the encrypted key with his private key, decrypts the ciphertext with the secret key.



encrypted key

decrypt

⟶

private key

secret key

ciphertext

decrypt

⟶

secret key

message

Standards

ANSI

X9.30,.31: DSS, RSA

NIST

DES, DSS, SHS

Key management, certification forthcoming

CCITT

X.400, X.500

ISO/IEC

IS 9796: RSA-oriented signature scheme

Standards (cont'd)

Internet

- Privacy-Enhanced Mail: RSA, DES, MD5
- SNMP: MD5

RSADSI *et al*

- PKCS (Public-Key Cryptography Standards)

***Also:* French Banking, Standards Australia, ...**

Conclusions

Basic concepts, various algorithms, many standards

- Secret key, public key, message digest
- RSA, DES, MD5, DSS, ...
- ANSI, NIST, ISO, PKCS, ...

Powerful applications

- Digital signatures, digital envelopes
- Hybrid cryptography combines benefits