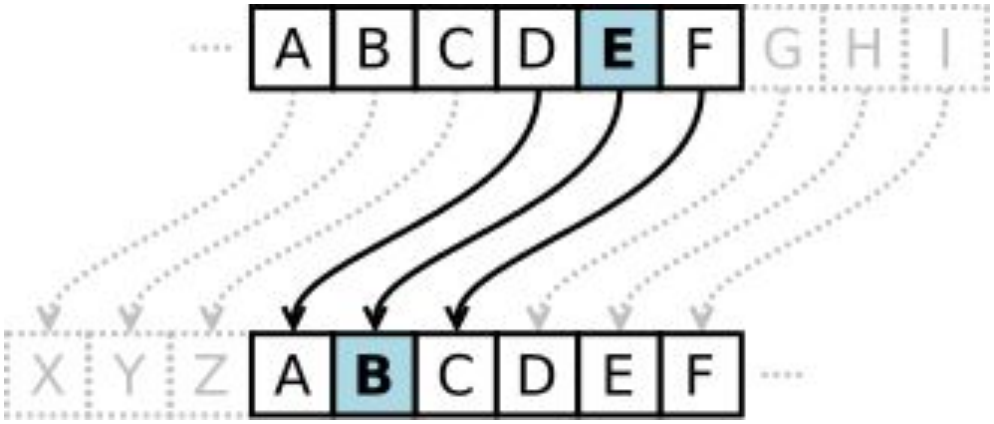
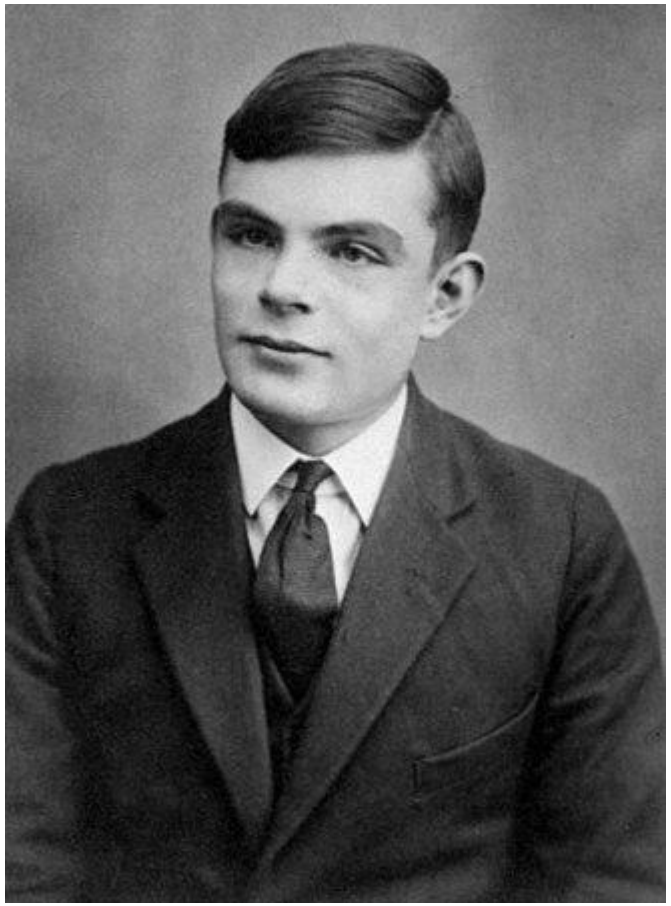
Computer Security: Principles and Practice

Chapter 2 – Cryptographic Tools

Historical Facts



Ceasar Cipher: private correspondence (~50BC)



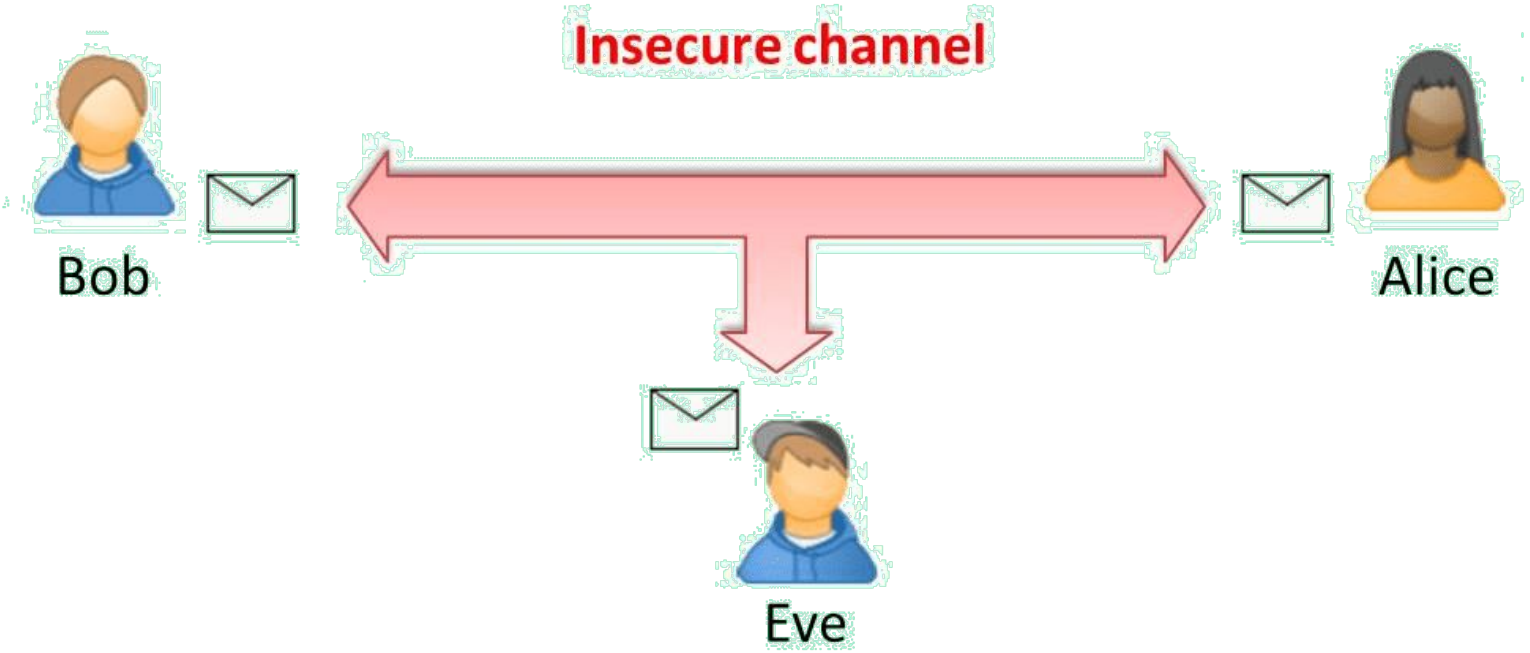
Alan Turing: decription of German's ciphers during WWII (1940s)

Cryptographic Tools

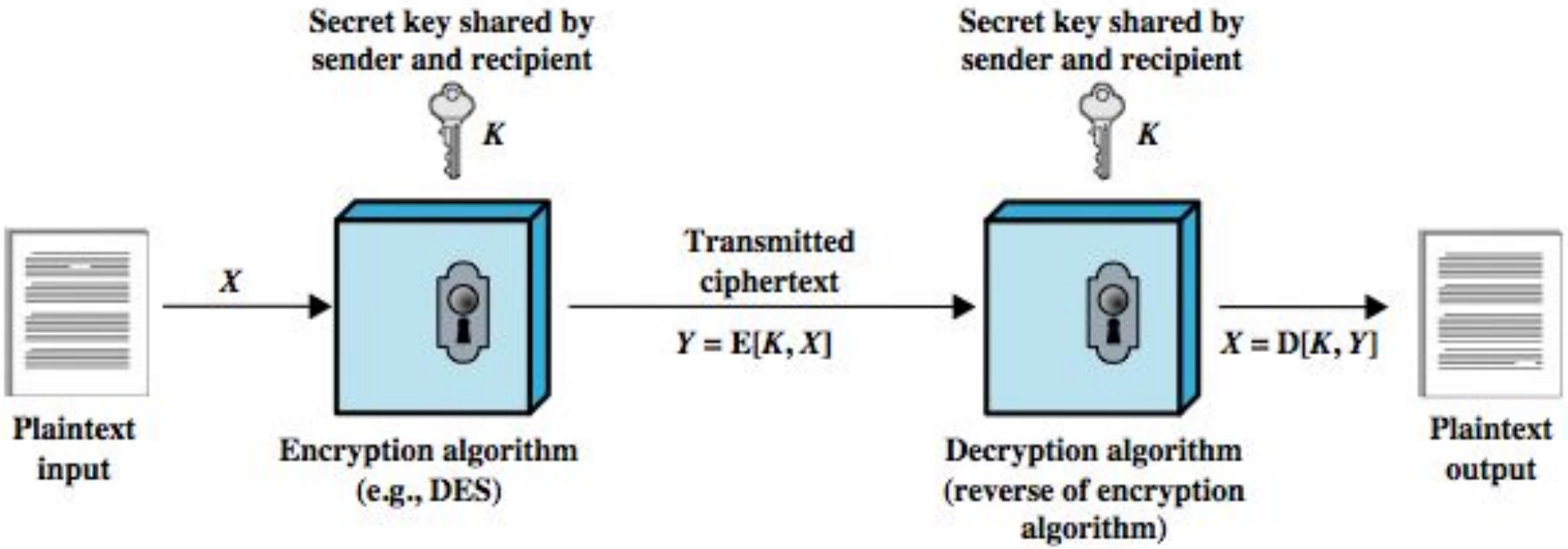
- cryptographic algorithms important element in security services
- review various types of elements
  - symmetric encryption
  - public-key (asymmetric) encryption
  - secure hash functions
- example of encryption

Symmetric Encryption

Symmetric Encryption



Symmetric Encryption

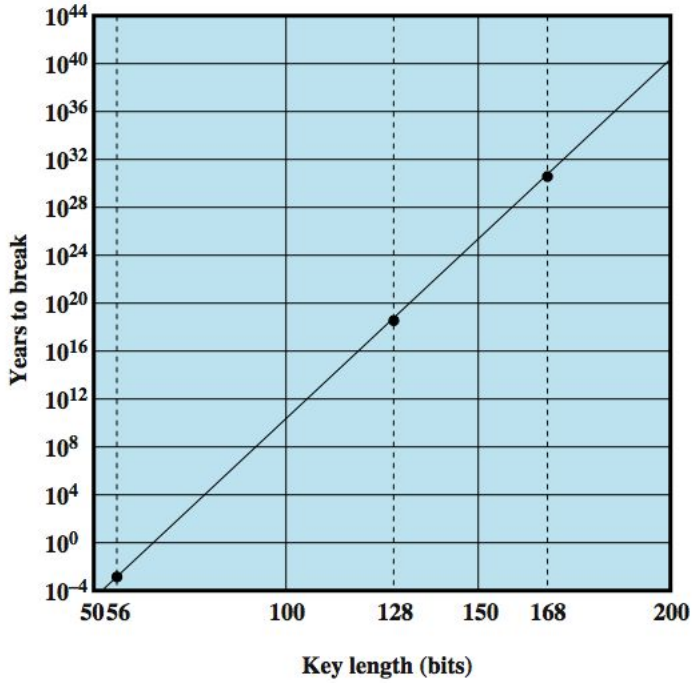


Attacking Symmetric Encryption

- cryptanalysis
  - rely on nature of the algorithm
  - plus some knowledge of plaintext characteristics
  - even some sample plaintext-ciphertext pairs
  - exploits characteristics of algorithm to deduce specific plaintext or key
- brute-force attack
  - try all possible keys on some ciphertext until get an intelligible translation into plaintext

Exhaustive Key Search

Key Size (bits)	Number of Alternative Keys	Time Required at 1 Decryption/μs	Time Required at 10^6 Decryptions/μs
32	$2^{32} = 4.3 \times 10^9$	$2^{31}\ \mu s = 35.8$ minutes	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	$2^{55}\ \mu s = 1142$ years	10.01 hours
128	$2^{128} = 3.4 \times 10^{38}$	$2^{127}\ \mu s = 5.4 \times 10^{24}$ years	5.4×10^{18} years
168	$2^{168} = 3.7 \times 10^{50}$	$2^{167}\ \mu s = 5.9 \times 10^{36}$ years	5.9×10^{30} years
26 characters (permutation)	$26! = 4 \times 10^{26}$	$2 \times 10^{26}\ \mu s = 6.4 \times 10^{12}$ years	6.4×10^6 years



Symmetric Encryption Algorithms

	DES	Triple DES	AES
Plaintext block size (bits)	64	64	128
Ciphertext block size (bits)	64	64	128
Key size (bits)	56	112 or 168	128, 192, or 256

DES = Data Encryption Standard
AES = Advanced Encryption Standard

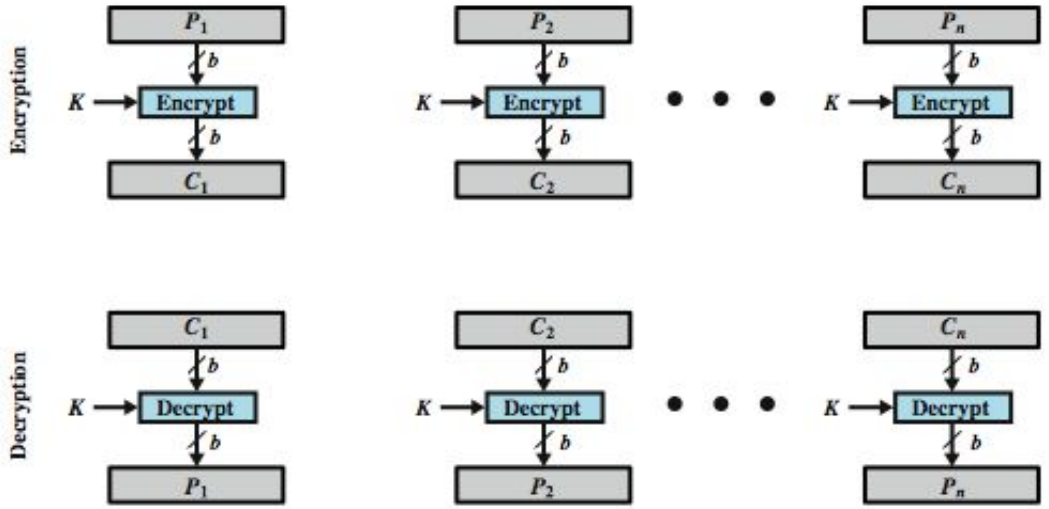
DES and Triple-DES

- Data Encryption Standard (DES) is the most widely used encryption scheme
  - uses 64 bit plaintext block and 56 bit key to produce a 64 bit ciphertext block
  - concerns about algorithm & use of 56-bit key
- Triple-DES
  - repeats basic DES algorithm three times
  - using either two or three unique keys
  - much more secure but also much slower

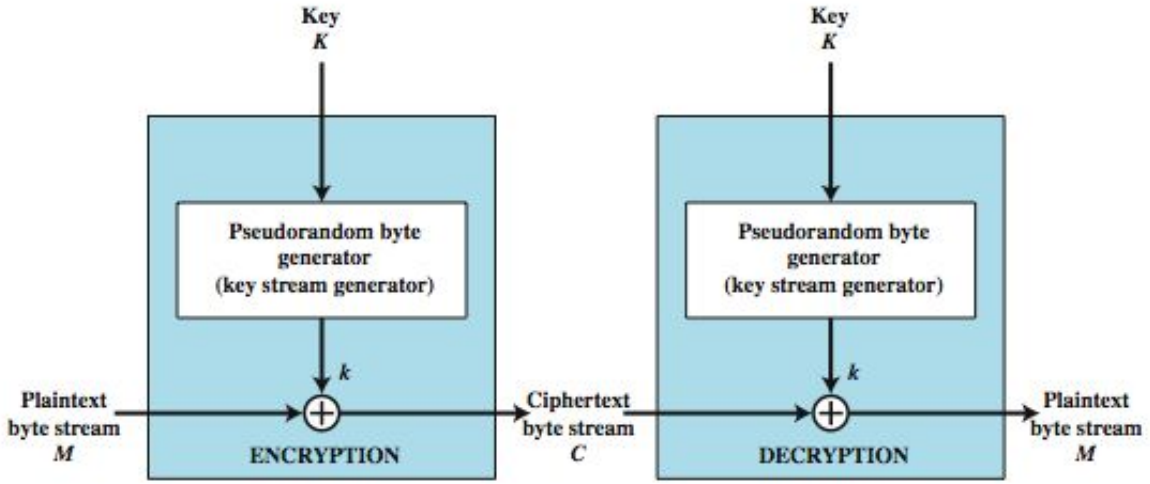
Advanced Encryption Standard (AES)

- needed a better replacement for DES
- NIST called for proposals in 1997
- selected Rijndael in Nov 2001
- published as FIPS 197
- symmetric block cipher
- uses 128 bit data & 128/192/256 bit keys
- now widely available commercially

Block vs. Stream Ciphers



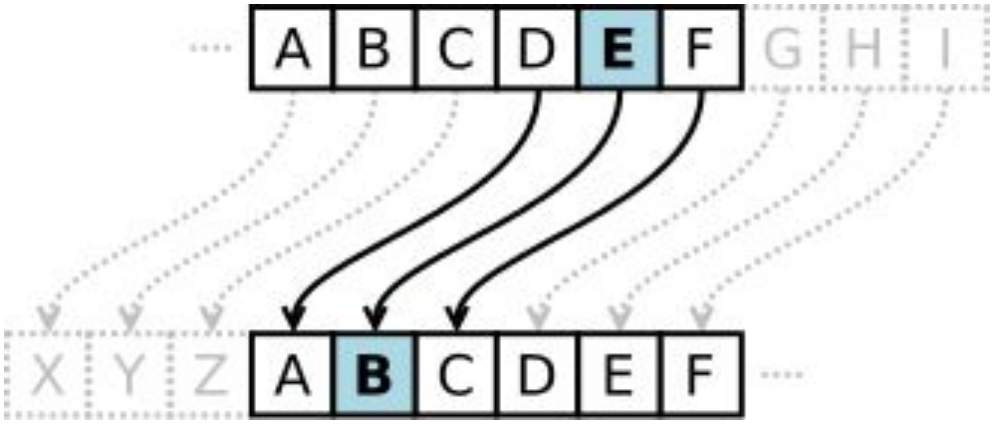
(a) Block cipher encryption (electronic codebook mode)



(b) Stream encryption

Example 1 - Caesar Cipher

- Substitution cipher
  - the alphabet is shifted
  - one of the easiest ciphers (and not really secure)



Example 1 - Caesar Cipher

- cyphertext:
  “QEB NRFZH YOLTK CLU GRJMP LSBO QEB IXWV ALD”
- Any ides?

Example 1 - Caesar Cipher

- cyphertext:
  “QEB NRFZH YOLTK CLU GRJMP LSBO QEB IXWV ALD”
- solution: try all the possible combinations of alphabets (shifts)
  - cryptanalysis + bruteforce in this case is easier then cryptanalysis
- plaintext: “THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG”

Example 2 - Mixed Alphabet Cipher

- stronger then Ceasar Chipher
- the cipher's alphabet is given by a random mapping with the letters

Example 2 - Mixed Alphabet Cipher

- **Question:** What about brute force?

Example 2 - Mixed Alphabet Cipher

- **Question:** What about brute force?
  - not a good approach this time
  - e.g., with English Alphabet (26 letters), all the possible combinations are 26!
- Cryptanalysis is better
  - we can rely on the nature of the text

Example 2 - Mixed Alphabet Cipher

- Ciphertext: “O'J Q NGXHU JQH”

Example 2 - Mixed Alphabet Cipher

- Ciphertext: “O'J Q NGXHU JQH”
- and now what???

Example 2 - Mixed Alphabet Cipher

- Ciphertext: “O'J Q NGXHU JQH”
- we can use some info:
  - it’s English, must follow some syntactic rules
  - we can also use statistic information about the language
    - unigram, bigram, trigram probabilities
  - be smart!
    - O’J must be something simple such as “I’M” or “I’D”
    - “Q” must be a vocal (e.g., “A”)
- plaintext: “I’m a young man”

Example 11

“Living is easy with eyes closed

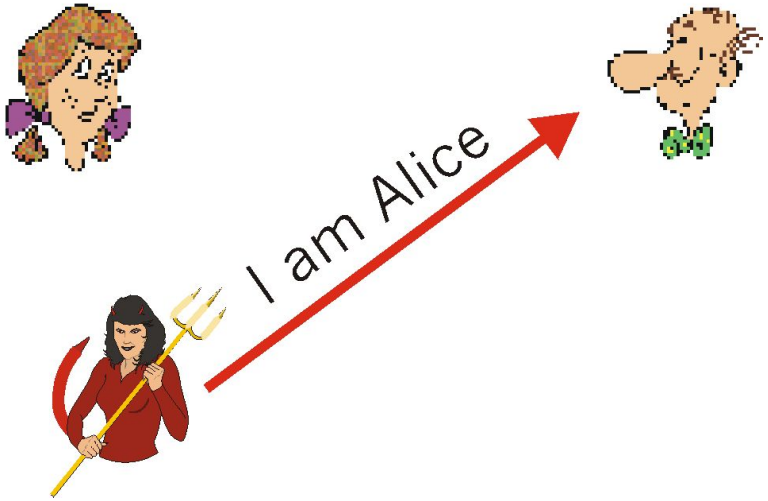
Misunderstanding all you see”

John Lennon - Strawberry Field Forever

Example 11

- Sometimes the encryption is not given to you in a clear format
  - check if it is in an ASCII format
- For example the cyphertext could be written in different “ways”
  - e.g., hex: “HI” -> “48 49”
  - e.g., binary, base64 (widely used in web communications)

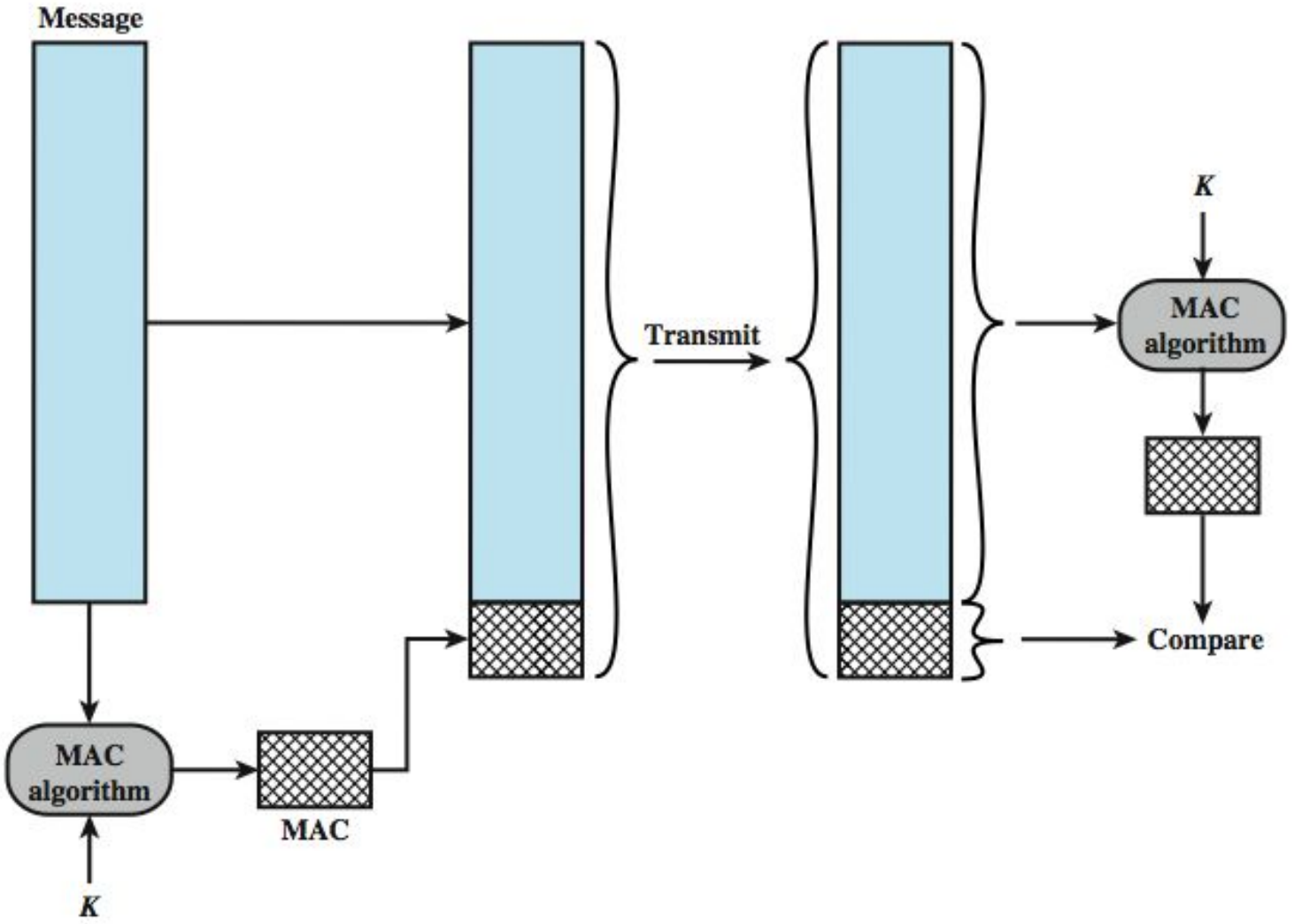
Message Authentication



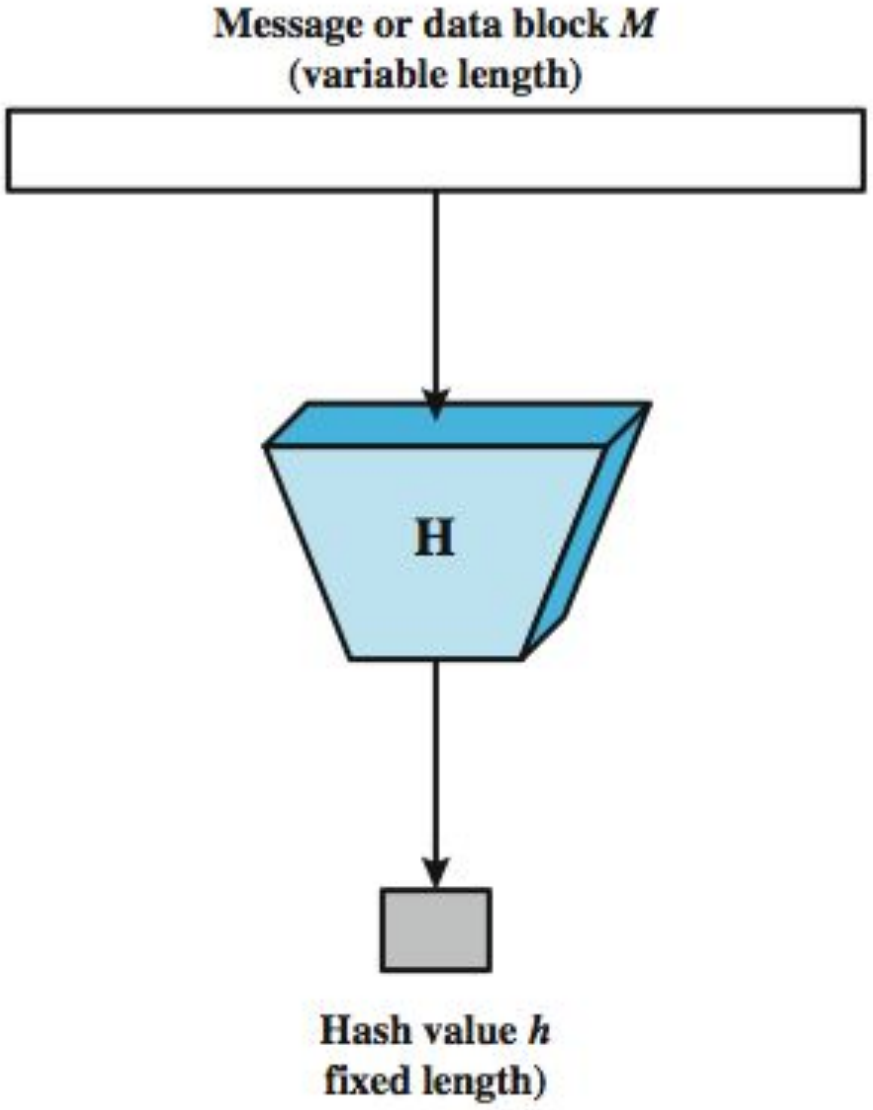
Message Authentication

- protects against active attacks
- verifies received message is authentic
  - contents unaltered
  - from authentic source
  - timely and in correct sequence
- can use conventional encryption
  - only sender & receiver have key needed
- or separate authentication mechanisms
  - append authentication tag to cleartext message

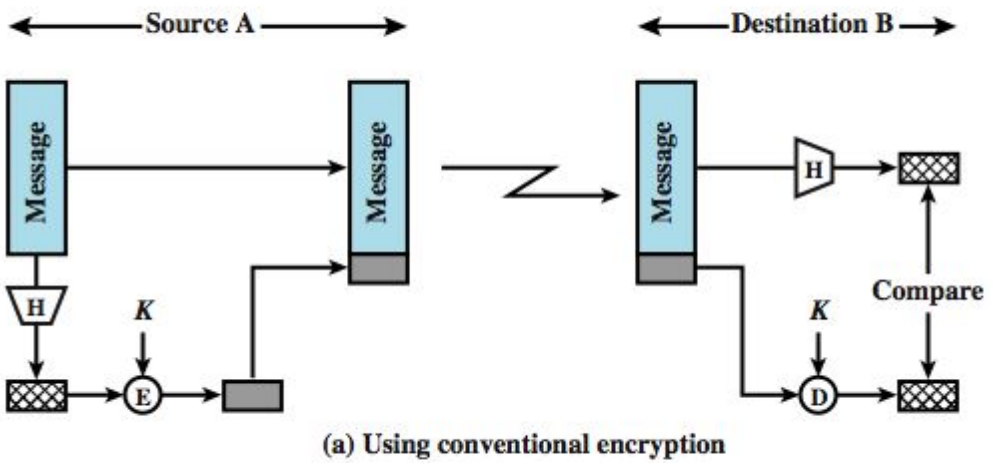
Message Authentication Codes



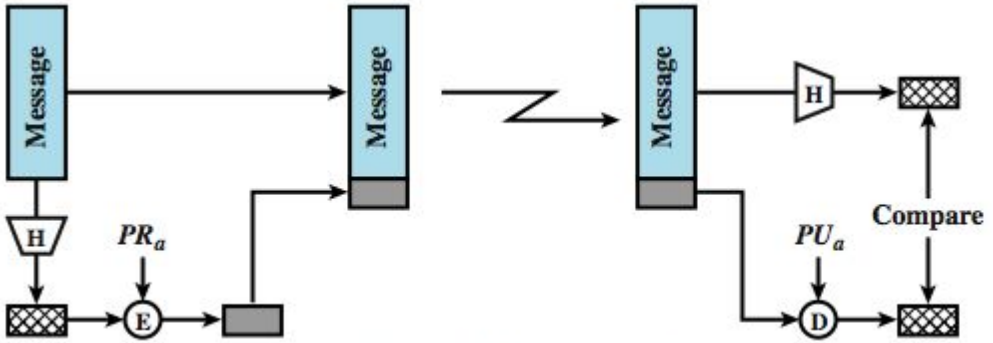
Secure Hash Functions



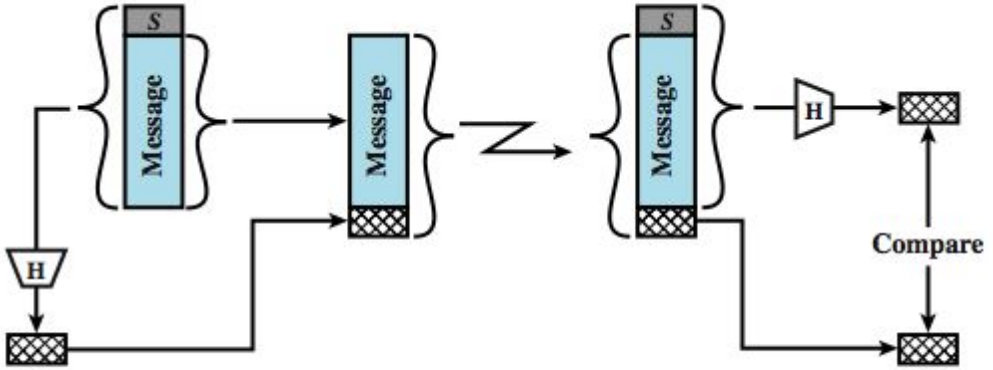
Message Auth



(a) Using conventional encryption



(b) Using public-key encryption



(c) Using secret value

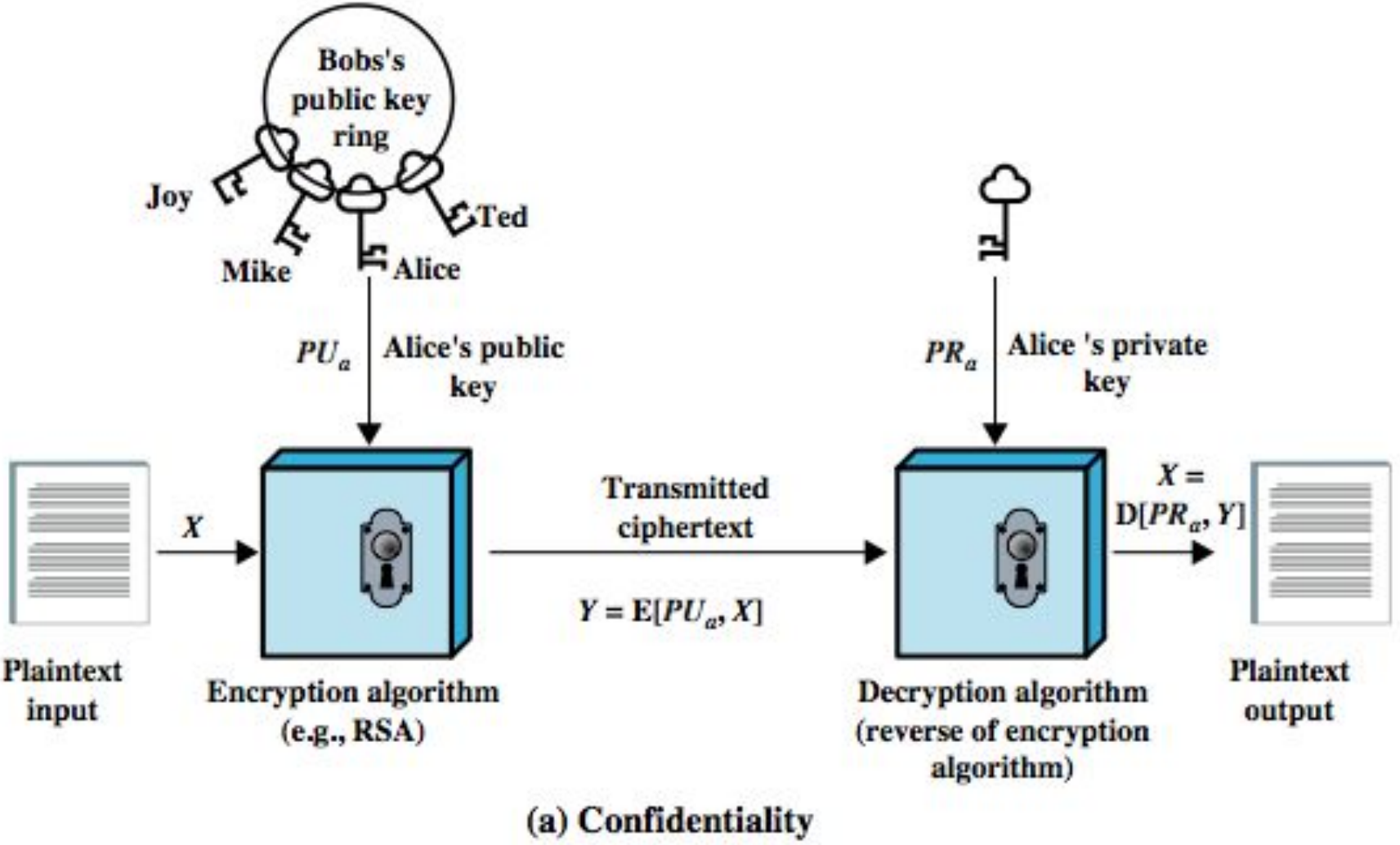
Hash Function Requirements

- applied to any size data
- H produces a fixed-length output.
- H(x) is relatively easy to compute for any given x
- one-way property
  - computationally infeasible to find x such that H(x) = h
- weak collision resistance
  - (given x) computationally infeasible to find $y \neq x$ such that H(y) = H(x)
- strong collision resistance
  - computationally infeasible to find any pair (x, y) such that H(x) = H(y)

Hash Functions

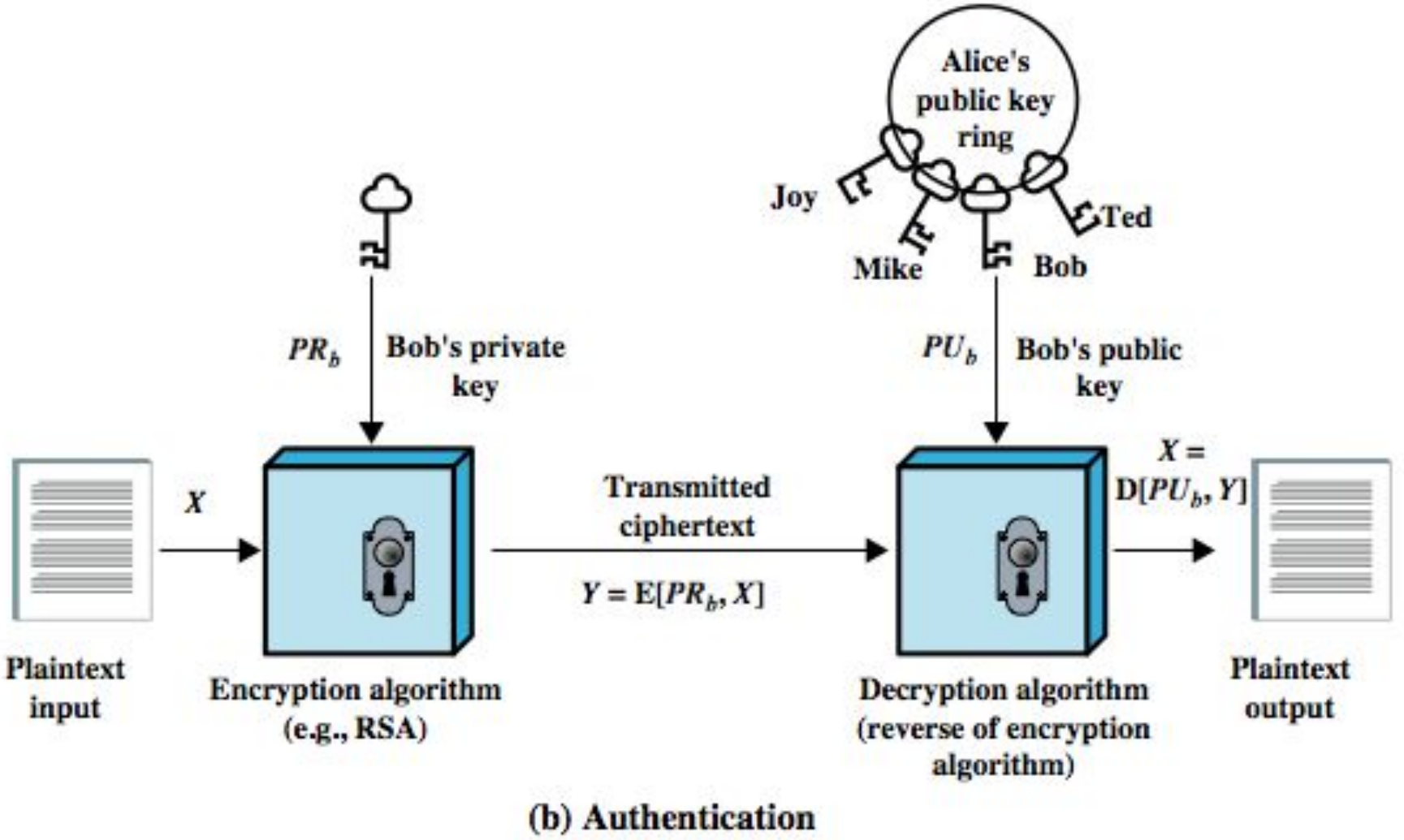
- two attack approaches
  - cryptanalysis
    - exploit logical weakness in alg
  - brute-force attack
    - trial many inputs
    - strength proportional to size of hash code
- SHA most widely used hash algorithm
  - SHA-1 gives 160-bit hash
  - more recent SHA-256, SHA-384, SHA-512 provide improved size and security

Public Key Encryption



(a) Confidentiality

Public Key Authentication



(b) Authentication

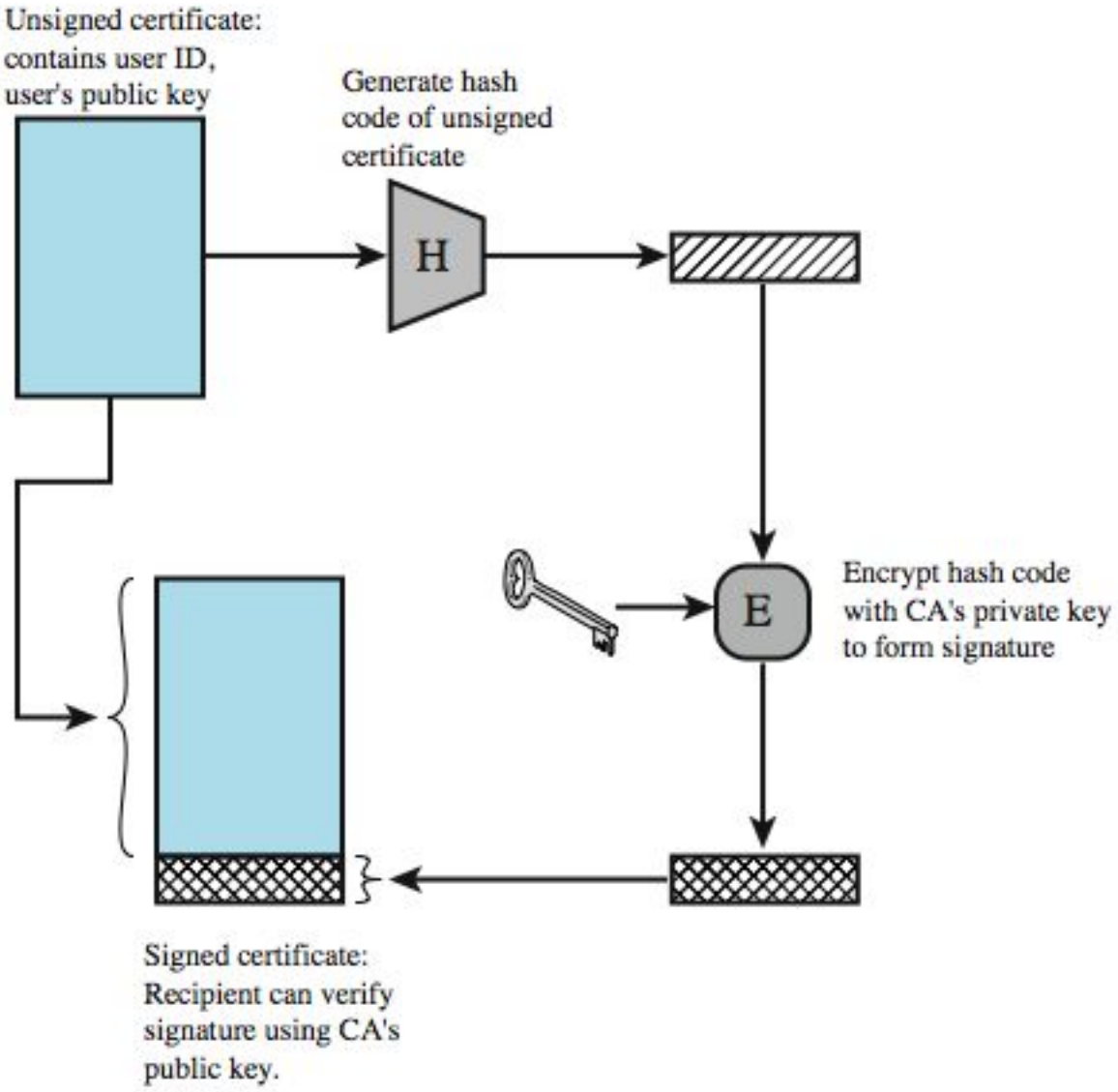
Public Key Requirements

1. computationally easy to create key pairs
2. computationally easy for sender knowing public key to encrypt messages
3. computationally easy for receiver knowing private key to decrypt ciphertext
4. computationally infeasible for opponent to determine private key from public key
5. computationally infeasible for opponent to otherwise recover original message
6. useful if either key can be used for each role

Public Key Algorithms

- RSA (Rivest, Shamir, Adleman)
  - developed in 1977
  - only widely accepted public-key encryption alg
  - given tech advances need 1024+ bit keys
- Diffie-Hellman key exchange algorithm
  - only allows exchange of a secret key
- Digital Signature Standard (DSS)
  - provides only a digital signature function with SHA-1
- Elliptic curve cryptography (ECC)
  - new, security like RSA, but with much smaller keys

Public Key Certificates



Random Numbers

- random numbers have a range of uses
- requirements:
  - randomness
    - based on statistical tests for uniform distribution and independence
  - unpredictability
    - successive values not related to previous
    - clearly true for truly random numbers
    - but more commonly use generator

Pseudorandom vs. Random Numbers

- often use algorithmic technique to create pseudorandom numbers
  - which satisfy statistical randomness tests
  - but likely to be predictable
- true random number generators use a nondeterministic source
  - e.g. radiation, gas discharge, leaky capacitors
  - increasingly provided on modern processors

Practical Application: Encryption of Stored Data

- common to encrypt transmitted data
- much less common for stored data
  - which can be copied, backed up, recovered
- approaches to encrypt stored data:
  - back-end appliance
  - library based tape encryption
  - background laptop/PC data encryption

Summary

- introduced cryptographic algorithms
- symmetric encryption algorithms for confidentiality
- message authentication & hash functions
- public-key encryption
- digital signatures and key management
- random numbers