Security in Computer Networks

Raj Jain
Washington University in Saint Louis
Saint Louis, MO 63130
Jain@wustl.edu

Audio/Video recordings of this lecture are available on-line at:

http://www.cse.wustl.edu/~jain/cse473-11/

1. Secret Key Encryption
2. Public Key Encryption

Not Covered: Hash Functions, Digital Signature, Digital Certificates, IPSec, VPN, Firewalls, Intrusion Detection Email Security, SSL, IKE, WEP

Note: This class lecture is based on Chapter 8 of the textbook (Kurose and Ross) and the figures provided by the authors.

Security Requirements

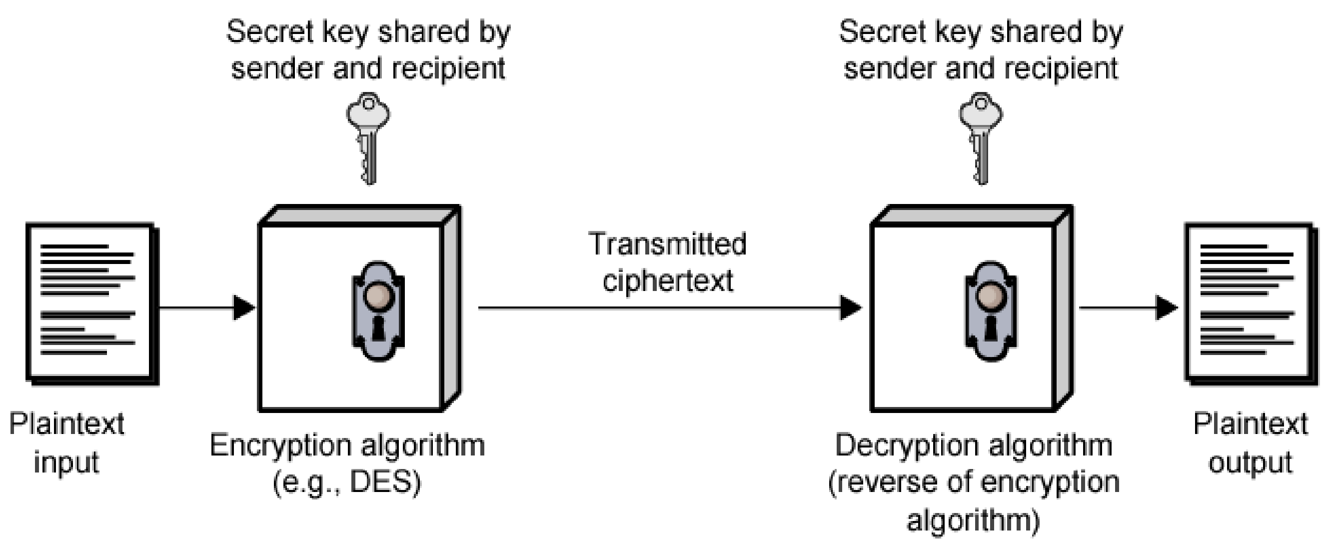
- **Integrity**: Received = sent?
- **Availability**: Legal users should be able to use.
  Ping continuously ⇒ No useful work gets done.
- **Confidentiality and Privacy**:
  No snooping or wiretapping
- **Authentication**: You are who you say you are.
  A student at Dartmouth posing as a professor canceled the exam.
- **Authorization** = Access Control
  Only authorized users get to the data
- **Non-repudiation**: Neither sender nor receiver can deny the existence of a message

Secret Key Encryption

1. Secret Key Encryption
2. Block Encryption
3. Cipher Block Chaining (CBC)
4. DES, 3DES, AES
5. Stream Cipher: RC4
6. Key Distribution

Secret Key Encryption

- Also known as symmetric key encryption
- Encrypted_Message = Encrypt(Key, Message)
- Message = Decrypt(Key, Encrypted_Message)
- Example: Encrypt = division
- 433 = 48 R 1 (using divisor of 9)



Secret Key: A Simple Example

- **Substitution**: Substituting one thing for another
- **Monoalphabetic**: substitute one letter for another

plaintext: abcdefghijklmnopqrstuvwxyz

↓ ↓

ciphertext: mnbvcxzasdfghjklpoiuytrewq

E.g.:

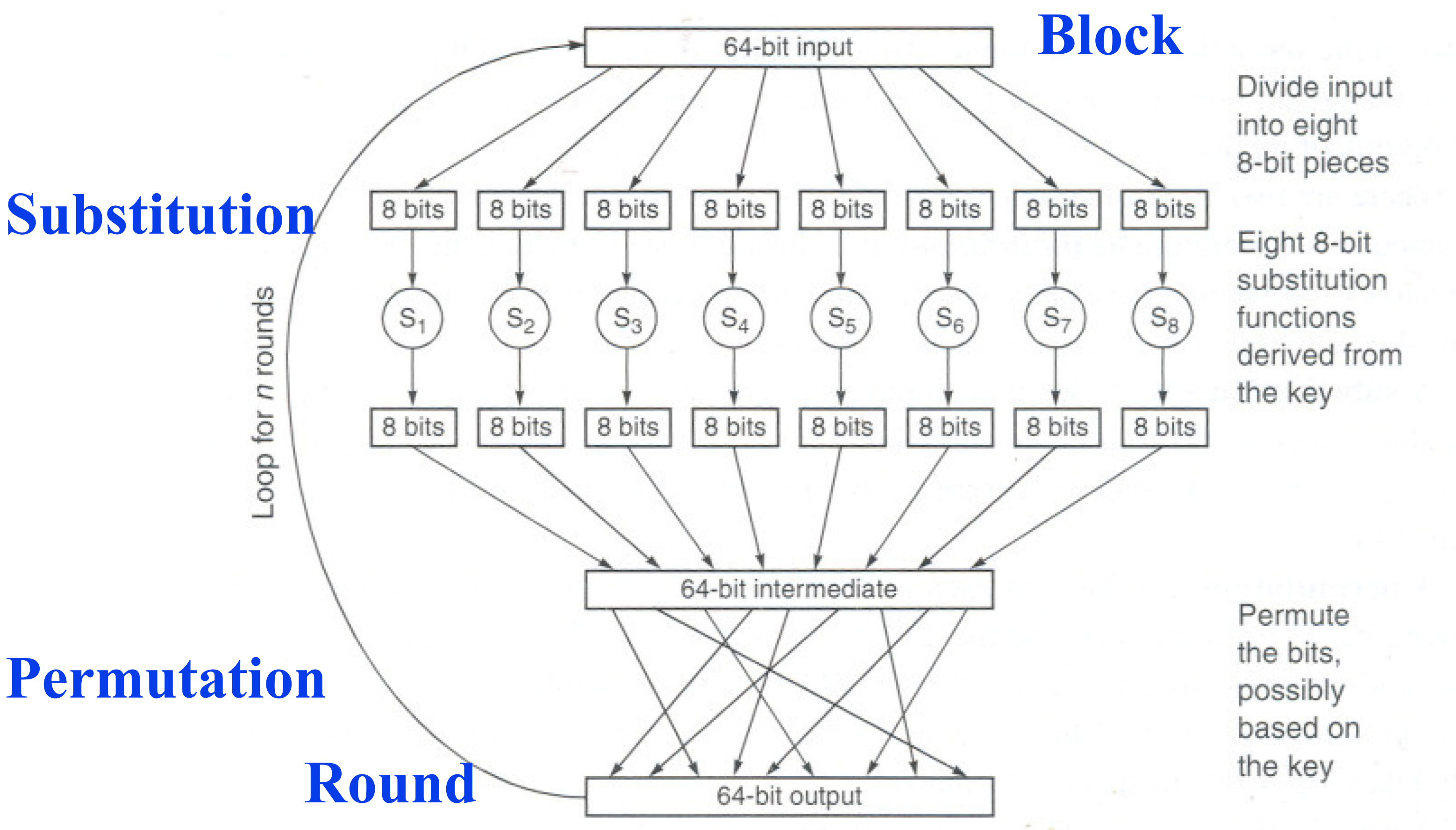
Plaintext: bob. i love you. alice

ciphertext: nkn. s gktc wky. mgsbc

- **Polyalphabetic**: Use multiple substitutions C1, C2, …
  Substitution selected depends upon the position
  ⇒Same letter coded differently in different position

Block Encryption

- Block Encryption

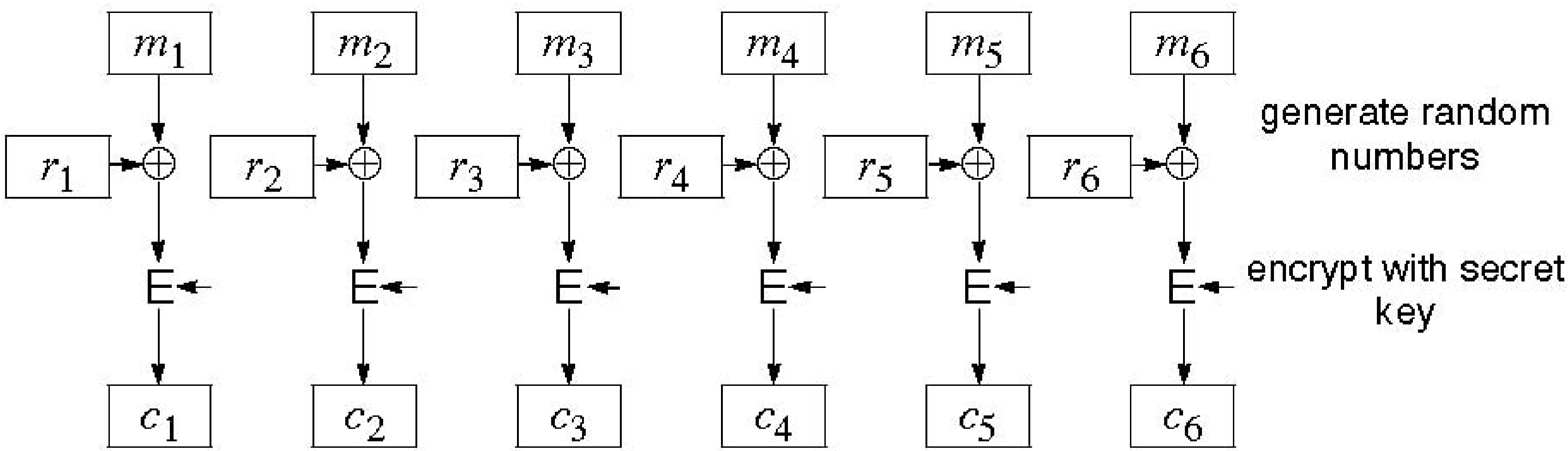


Block Encryption (Cont)

- Short block length ⇒ tabular attack
- 64-bit block
- Transformations:
  - Substitution: replace k-bit input blocks with k-bit output blocks
  - Permutation: move input bits around. $1 \rightarrow 13$, $2 \rightarrow 61$, etc.
- Round: Substitution round followed by permutation round and so on. Diffusion + Confusion.

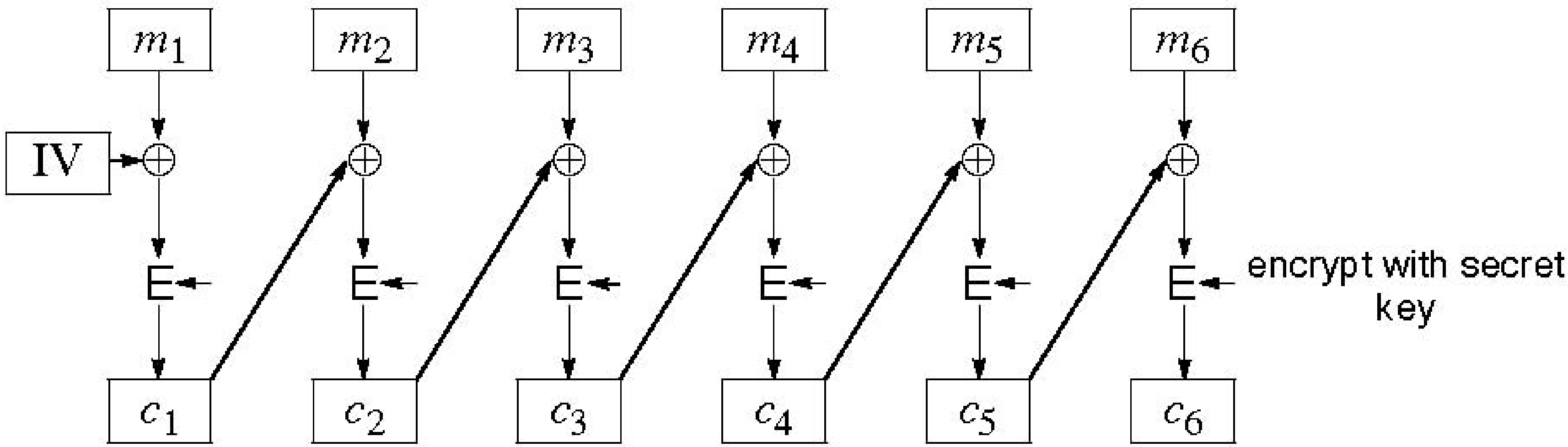
Cipher Block Chaining (CBC)

- Goal: Same message encoded differently
- Add a random number before encoding



CBC (Cont)

- Use C_i as random number for i+1



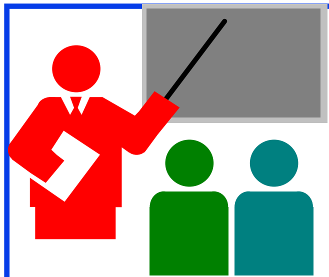
- Need Initial Value (IV)
- no IV ⇒ Same output for same message
  ⇒ one can guess changed blocks
- Example: Continue Holding, Start Bombing

DES and 3DES

- Data Encryption Standard (DES)
  - 64 bit plain text blocks, 56 bit key
  - Broken in 1998 by Electronic Frontier Foundation
- Triple DES (3DES)
  - Uses 2 or 3 keys and 3 executions of DES
  - Effective key length 112 or 168 bit
  - Block size (64 bit) too small ⇒ Slow

Advanced Encryption Standard (AES)

- Designed in 1997-2001 by National Institute of Standards and Technology (NIST)
- Federal information processing standard (FIPS 197)
- Symmetric block cipher, Block length 128 bits
- Key lengths 128, 192, and 256 bits



Secret Key Encryption: Review

1. Secret key encryption requires a shared secret key
2. Block encryption, e.g., DES, 3DES, AES break into fixed size blocks and encrypt
3. CBC is one of many modes are used to ensure that the same plain text results in different cipher text.
4. Stream Cipher, e.g., RC4, generate a random stream and xor to the data
5. Key distribution center can be used to exchange session keys

Home Exercises

- Try but do not submit
- Review questions R1, R2, R6
- Problems P1, P2, P3, P4, P5, P6
- Read pages 687-698 of the textbook

Homework 8A

- Problem P6: Consider 3-bit block cipher in Table 8.1.

Plain	000	001	010	011	100	101	110	111
Cipher	110	111	101	100	011	010	000	001

- Suppose the plaintext is 100100100.

(a) Initially assume that CBC is not used. What is the resulting ciphertext?

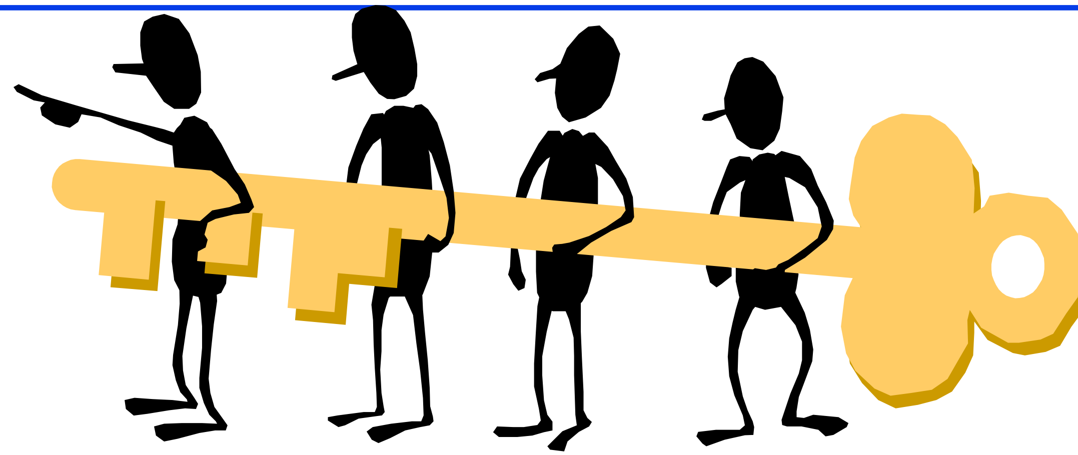
(b) Suppose Trudy sniffs the cipher text. Assuming she knows that a 3-bit block cipher without CBC is being employed (but doesn't know the specific cipher), what can she surmise?

(c) Now suppose that CBC is used with IV-111. What is the resulting ciphertext?

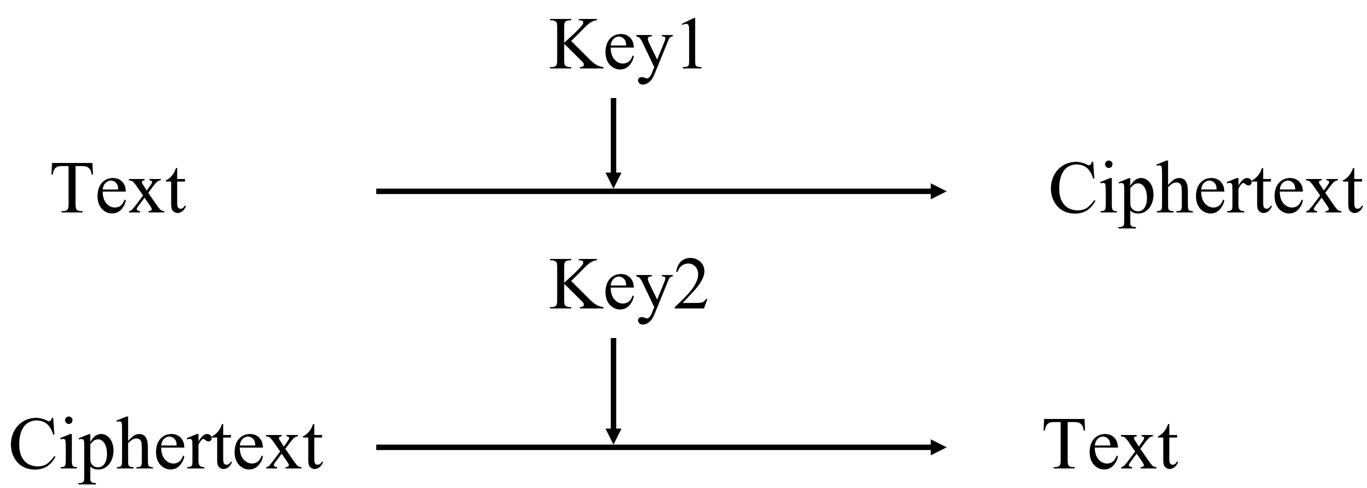
Public Key Encryption

1. Public Key Encryption
2. Modular Arithmetic
3. RSA Public Key Encryption
4. Confidentiality
5. Diffie-Hellman Key Agreement
6. Hash Functions: MD5, SHA-1
7. Message Authentication Code (MAC)
8. Digital Signature
9. Digital Certificates

Public Key Encryption

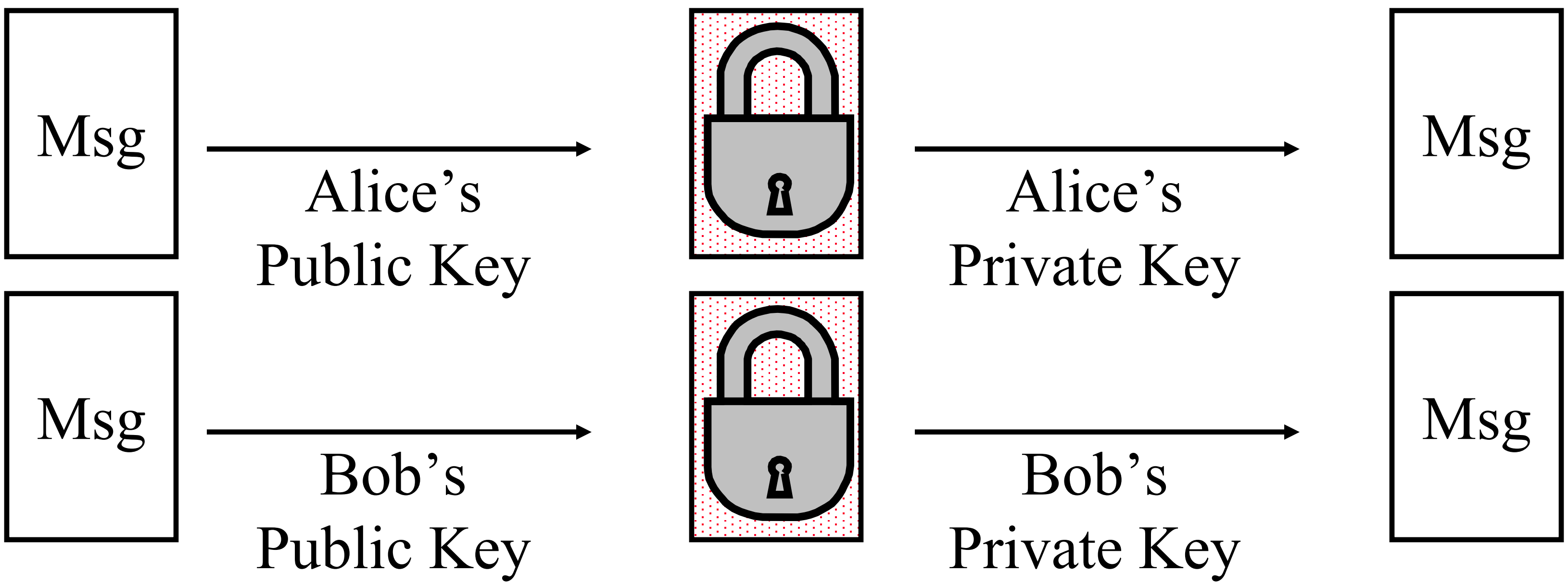


- Invented in 1975 by Diffie and Hellman
- Encrypted_Message = Encrypt(Key1, Message)
- Message = Decrypt(Key2, Encrypted_Message)



Public Key (Cont)

- One key is private and the other is public
- Message = Decrypt(Public_Key, Encrypt(Private_Key, Message))
- Message = Decrypt(Private_Key, Encrypt(Public_Key, Message))



Public Key Encryption Method

- RSA: Encrypted_Message = m^3 mod 187
- Message = $\text{Encrypted\_Message}^{107}$ mod 187
- Key1 = <3,187>, Key2 = <107,187>
- Message = 5
- Encrypted Message = $5^3 = 125$
- Message = 125^{107} mod 187 = 5
  = $125^{(64+32+8+2+1)}$ mod 187
  = $\{(125^{64}$ mod 187)(125^{32} mod 187)...
  (125^2 mod 187)(125 mod 187)$\}$ mod 187

Modular Arithmetic

- $xy \bmod m = (x \bmod m)\,(y \bmod m) \bmod m$
- $x^4 \bmod m = (x^2 \bmod m)(x^2 \bmod m) \bmod m$
- $x^{ij} \bmod m = (x^i \bmod m)^j \bmod m$
- $125 \bmod 187 = 125$
- $125^2 \bmod 187 = 15625 \bmod 187 = 104$
- $125^4 \bmod 187 = (125^2 \bmod 187)^2 \bmod 187$
  $= 104^2 \bmod 187 = 10816 \bmod 187 = 157$
- $125^8 \bmod 187 = 157^2 \bmod 187 = 152$
- $125^{16} \bmod 187 = 152^2 \bmod 187 = 103$
- $125^{32} \bmod 187 = 103^2 \bmod 187 = 137$
- $125^{64} \bmod 187 = 137^2 \bmod 187 = 69$
- $125^{64+32+8+2+1} \bmod 187 = 69 \times 137 \times 152 \times 104 \times 125 \bmod 187$
  $= 18679128000 \bmod 187 = 5$

RSA Public Key Encryption

- Ron Rivest, Adi Shamir, and Len Adleman at MIT 1978
- Both plain text M and cipher text C
  are integers between 0 and n-1.
- Key 1 = {e, n},
  Key 2 = {d, n}
- $C = M^e \bmod n$
  $M = C^d \bmod n$
- How to construct keys:
  - Select two large primes: p, q, $p \neq q$
  - $n = p \times q$
  - Calculate $z = (p-1)(q-1)$
  - Select e, such that $\gcd(z, e) = 1$; $0 < e < z$
  - Calculate d such that $de \bmod z = 1$

RSA Algorithm: Example

- Select two large primes: p, q, $p \neq q$
  $p = 17, q = 11$
- $n = p \times q = 17 \times 11 = 187$
- Calculate $z = (p-1)(q-1) = 16x10 = 160$
- Select e, such that $gcd(z, e) = 1; 0 < e < z$
  say, $e = 7$
- Calculate d such that de mod z = 1
  - $160k+1 = 161, 321, 481, 641$
  - Check which of these is divisible by 7
  - 161 is divisible by 7 giving $d = 161/7 = 23$
- Key 1 = {7, 187}, Key 2 = {23, 187}

Homework 8B

Problem P8: Consider RSA with p=5, q=11

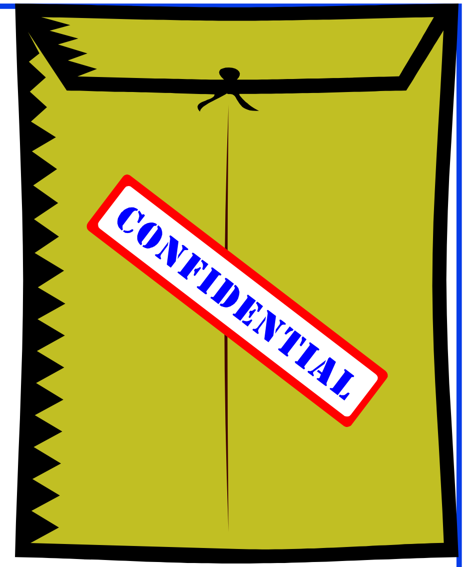
A. what are n and z

B. let e be 3. Why is this an acceptable choice for e?

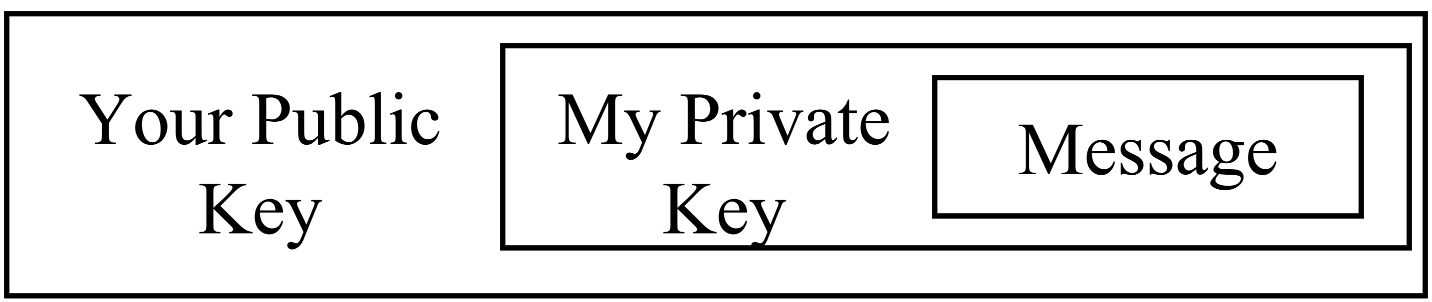
C. Find d such that de=1(mod z) and d<160

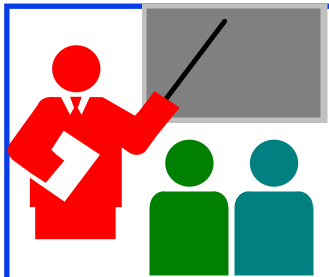
D. Encrypt the message m=8 using the key (n,e). Let c be the corresponding cipher text. Show all work including decryption.

Confidentiality



- User 1 to User 2:
- Encrypted_Message
  = Encrypt(Public_Key2,
  Encrypt(Private_Key1, Message))
- Message = Decrypt(Public_Key1,
  Decrypt(Private_Key2, Encrypted_Message)
  ⇒ Authentic and Private





Public Key Encryption: Review

1. Public Key Encryption uses two keys: Public and Private
2. RSA method is based on difficulty of factorization

Review Exercises

- Try but do not submit
- Review exercises:R7
- Problems: P7, P9, P10
- Read pages 699-704 of the textbook
- Sections 8.1 and 8.2

