Benha University

Faculty of Computers & Informatics

2nd Term (2013-2014) Final Exam
Class: 4th Year Students (CS)
Subject: Computer Security Methods

Date: 17/5/2014
Time: 3 hours

Answer the following questions.

Question 1[20 points]

1. Multiple Choice

1) If Alice has a message to send to Bob and she wants to encrypt the message using asymmetric cryptography so that no one other than Bob can read it, she does so by using Bob's public key.
   A) **TRUE** B) FALSE
2) An attraction of public key cryptography is that, if implemented properly, the algorithms generally run much faster than those for symmetric key cryptography.
   A) TRUE B) **FALSE**
3) Encrypt the message "BFCI" using autokey cipher with key=7. The cipher text will be
   A) JHMN B)JHHN C) **IGMN** D) None of them
4) Encrypt the plaintext 'how' using the affine algorithm using k1=5 and k2=7. The cipher text will be
   A) **QZN** B) QZH C) PQN D) QYM E) None of them
5) Consider the PlayFair cipher which has "playfair example" as key. The cipher corresponding to the plain text "Hide the goldi" will be
   A) BMOIZBXDNABX B) BNODZBXDNABE C) BHODZRXDNABE
   D) **BMODZBXDNABE** E) None of them

2- Fill in the blanks

1- __confusion______ hides the relationship between the cipher text and the key.

2-With a(n) __brute force____ attack the attacker attempts to create every possible password combination by systematically changing one character at a time and then using each newly generated password to access the system.

3-The simplest and most secure type of synchronous stream cipher is called __one time pad________, which uses a key stream that is randomly chosen for each encipherment.

4-A__P-box__ parallels the traditional transposition cipher for characters.

5-An _____S-box_____ can be thought of as a miniature of a substitution cipher.

Question 2[60 points]

1-Define the three security goals. List and describe security attacks that threaten security goals.

2-Distinguish between security services and security mechanisms.

3-State and explain four kinds of cryptanalysis attacks based on what is known to the attacker.

4- What are the components of a Modern Block Cipher? Explain why modern block ciphers need to be designed as substitution ciphers.

5-List and describe briefly four modes of operations and explain why modes of operation are needed (possibly use a diagram).

6-Alice needs to send the message "Enemy attacks to night" to Bob. Assume that Alice and Bob used the transposition-cipher encryption key (3,1,4,5,2). What is the decryption key? If the double transposition cipher is used, what is the cipher text?

7-Draw a block diagram showing a single round structure at the encryption site of DES algorithm and explain the main components and operations of a single round at the encryption site of DES algorithm.

8-Discuss the weaknesses in DES algorithm.

9- A) Briefly explain the idea behind the knapsack cryptosystem

B) Given the super increasing tuple b=[7,11,19,39,79,157,313], r =37, and modulus n=900, encrypt and decrypt the letter "g" using the knapsack crptosystem. Use [4 2 5 3 1 7 6] as the permutation table. (The 7-bit ASCII representation of "g" is $(1100111)_2$)

10-Consider an RSA Public Key Cryptosystem

A) Alice selects two prime numbers: p=5, q=11. **Compute n, and Φ(n) ?**

B) Alice selects her public exponent e = 3, **Is this choice for "e" valid? Why?**

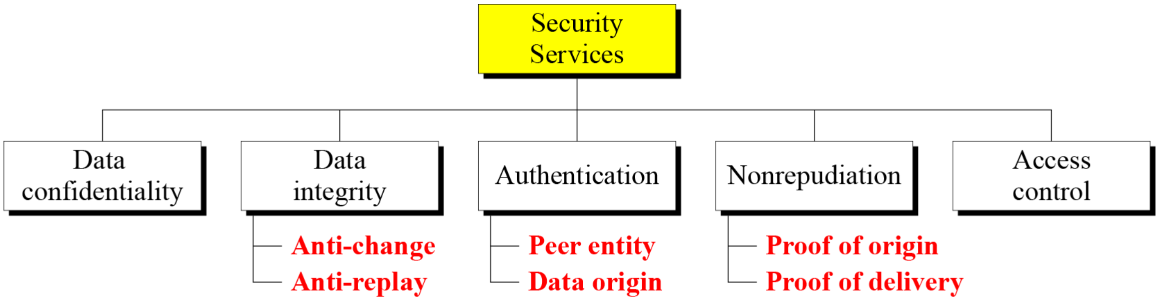
C) **Compute d** , the private exponent of Alice?

D) Now you want to send message M=4 to Alice. Encrypt your plaintext M using Alice public exponent. **What is the resulting cipher text C?**

E) Now Alice receives C, **verify that Alice can obtain M from C, using her private decryption exponent. (**use Fast Exponentiation /Square and Multiply method)

• **Confidentiality** (covers both data confidentiality and privacy): preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information.
• **Integrity** (covers both data and system integrity)**:** Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information.
• **Availability:** Ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information or an information system.

a processing or communication service provided by a system to give a specific kind of protection to system resources



- **a.k.a. control**
- **feature designed to detect, prevent, or recover from a security attack**
- **no single mechanism that will support all services required**
- **however one particular element underlies many of the security mechanisms in use:**
  - **cryptographic techniques**

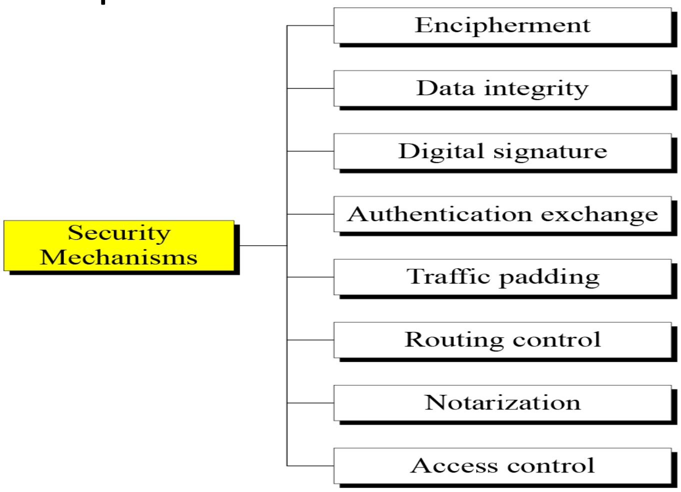
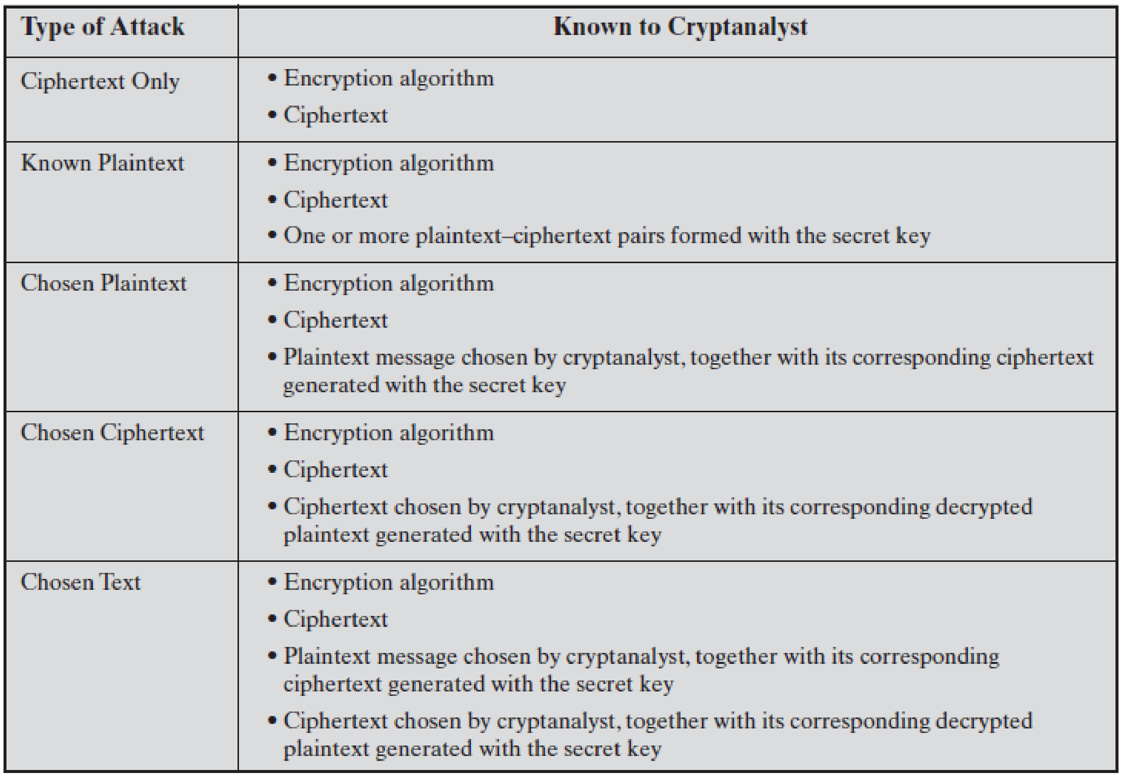


Table 2.1 Types of Attacks on Encrypted Messages



Type of Attack	Known to Cryptanalyst
Ciphertext Only	• Encryption algorithm • Ciphertext
Known Plaintext	• Encryption algorithm • Ciphertext • One or more plaintext–ciphertext pairs formed with the secret key
Chosen Plaintext	• Encryption algorithm • Ciphertext • Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key
Chosen Ciphertext	• Encryption algorithm • Ciphertext • Ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key
Chosen Text	• Encryption algorithm • Ciphertext • Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key • Ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key

A modern cipher is made of a combination of transposition units called (P-boxes) , substitution units called (S-boxex), and some other units.

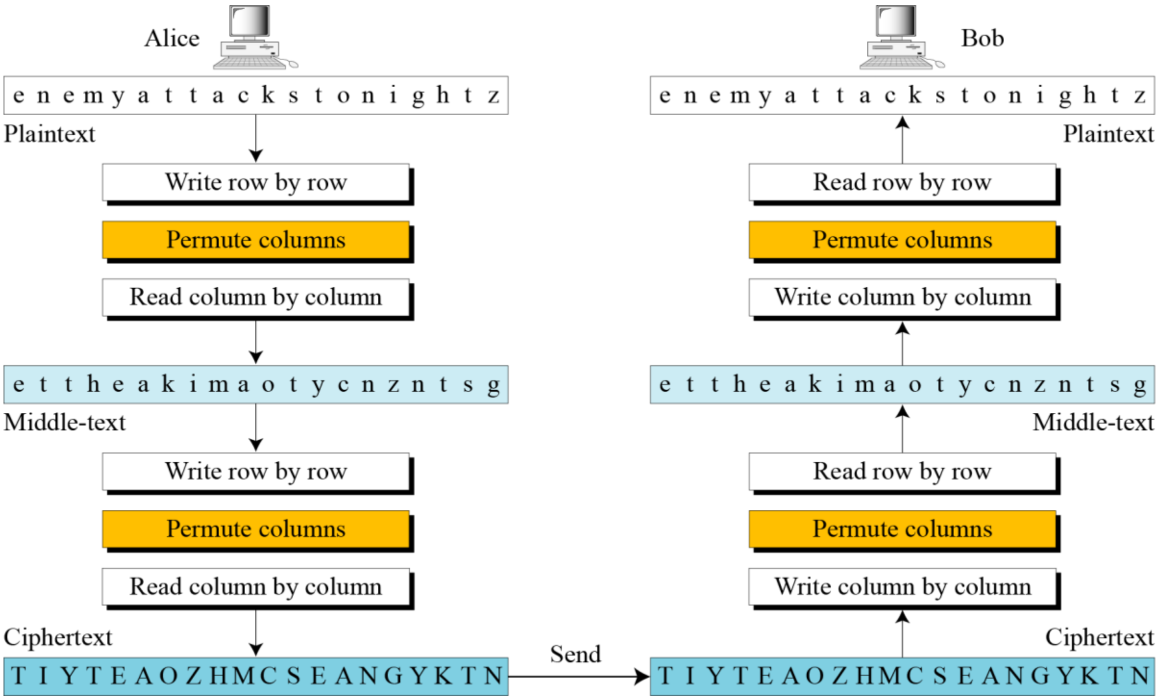
A modern block cipher can be designed to act as a substitution cipher or a transposition cipher.

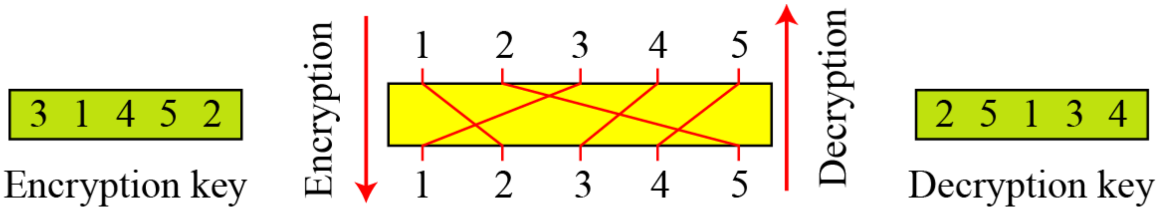
- If the cipher is designed as a **substitution cipher** , a 1-bit or 0-bit in the plaintext can be replaced by 0 or 1.
  - This means plaintext and cipher text can have different number of 1's
- If the cipher is designed as a **transposition cipher** , the bits are only reordered
  - There is the same number of 1's in the plaintext and in ciphertext

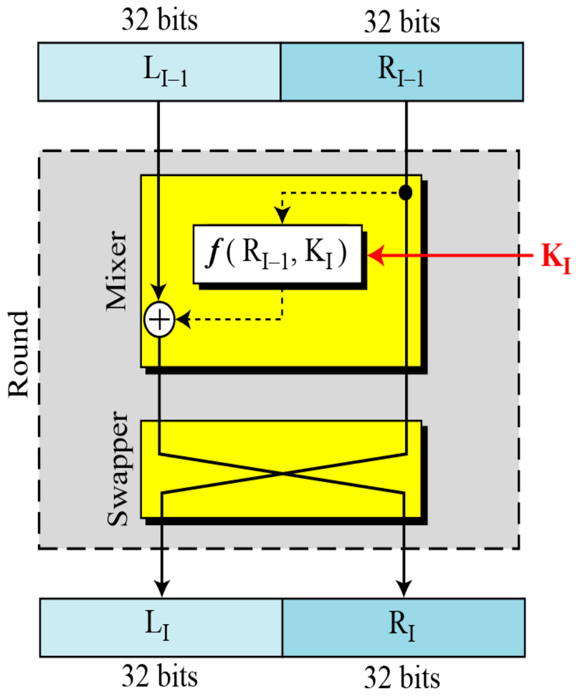
Table 8.1 *Summary of operation modes*

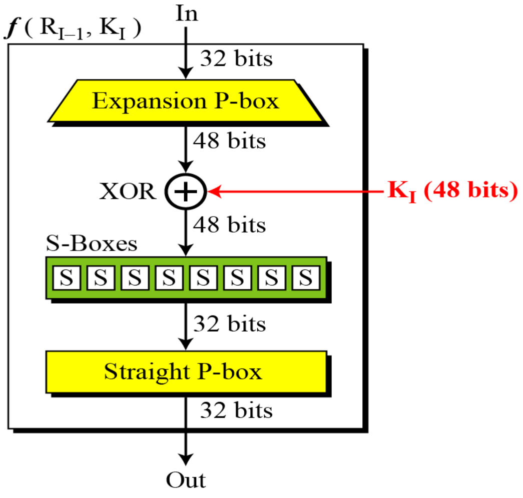
Operation Mode	*Description*	*Type of Result*	*Data Unit Size*
ECB	Each n-bit block is encrypted independently with the same cipher key.	Block cipher	n
CBC	Same as ECB, but each block is first exclusive-ored with the previous ciphertext.	Block cipher	n
CFB	Each r-bit block is exclusive-ored with an r-bit key, which is part of previous cipher text	Stream cipher	$r \leq n$
OFB	Same as CFB, but the shift register is updated by the previous r-bit key.	Stream cipher	$r \leq n$
CTR	Same as OFB, but a counter is used instead of a shift register.	Stream cipher	n

- A block cipher takes a fixed-length block of text of length b bits and a key as input and produces a b-bit block of ciphertext.
- If the amount of plaintext to be encrypted is greater than *b bits, then the block cipher can still be used by breaking the plaintext* up into b-bit blocks.
- To apply a block cipher in a variety of applications, five *modes of operation have been defined*
- a mode of operation is a technique for enhancing the effect of a cryptographic algorithm or adapting the algorithm for an application, such as applying a block cipher to a sequence of data blocks or a data stream.







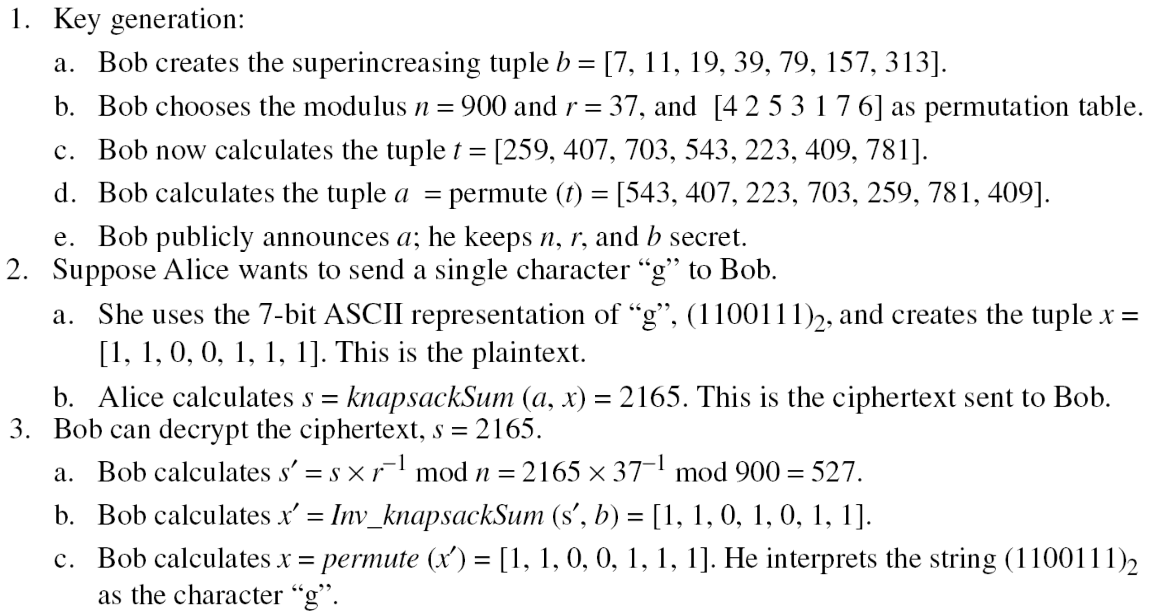


Weaknesses in DES Cipher Design

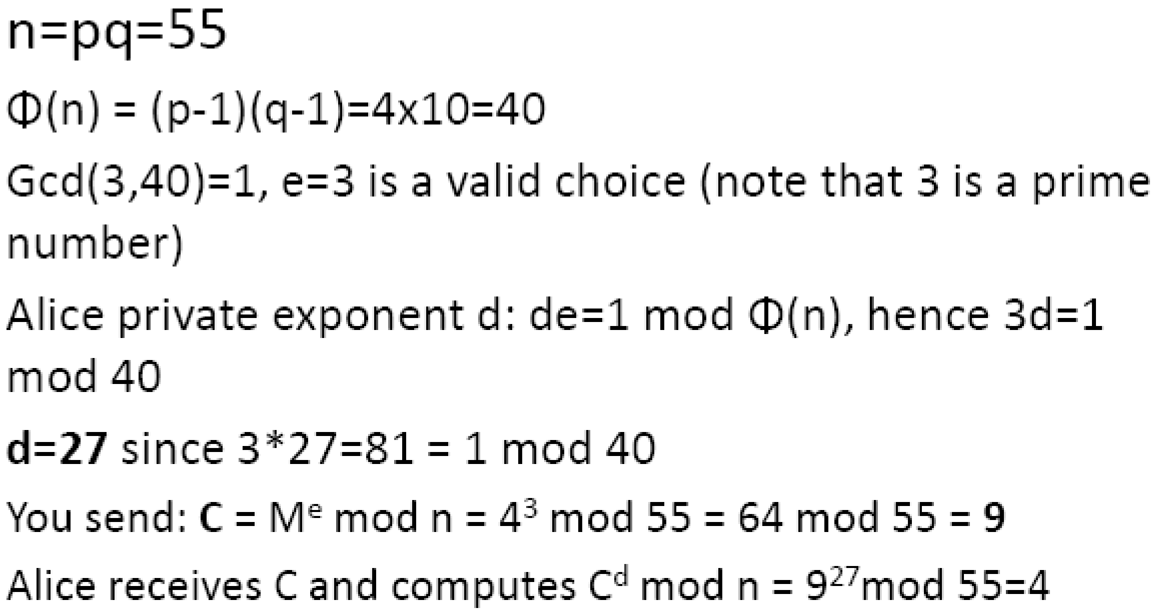
1. Weaknesses in S-boxes

2. Weaknesses in P-boxes

3. Weaknesses in Key



1. Key generation:
   a. Bob creates the superincreasing tuple $b = [7, 11, 19, 39, 79, 157, 313]$.
   b. Bob chooses the modulus $n = 900$ and $r = 37$, and [4 2 5 3 1 7 6] as permutation table.
   c. Bob now calculates the tuple $t = [259, 407, 703, 543, 223, 409, 781]$.
   d. Bob calculates the tuple a = permute $(t) = [543, 407, 223, 703, 259, 781, 409]$.
   e. Bob publicly announces a; he keeps n, r, and b secret.
2. Suppose Alice wants to send a single character “g” to Bob.
   a. She uses the 7-bit ASCII representation of “g”, $(1100111)_2$, and creates the tuple $x = [1, 1, 0, 0, 1, 1, 1]$. This is the plaintext.
   b. Alice calculates $s = knapsackSum\ (a, x) = 2165$. This is the ciphertext sent to Bob.
3. Bob can decrypt the ciphertext, $s = 2165$.
   a. Bob calculates $s' = s \times r^{-1} \bmod n = 2165 \times 37^{-1} \bmod 900 = 527$.
   b. Bob calculates $x' = Inv\_knapsackSum\ (s', b) = [1, 1, 0, 1, 0, 1, 1]$.
   c. Bob calculates $x = permute\ (x') = [1, 1, 0, 0, 1, 1, 1]$. He interprets the string $(1100111)_2$ as the character “g”.



n=pq=55

Φ(n) = (p-1)(q-1)=4x10=40

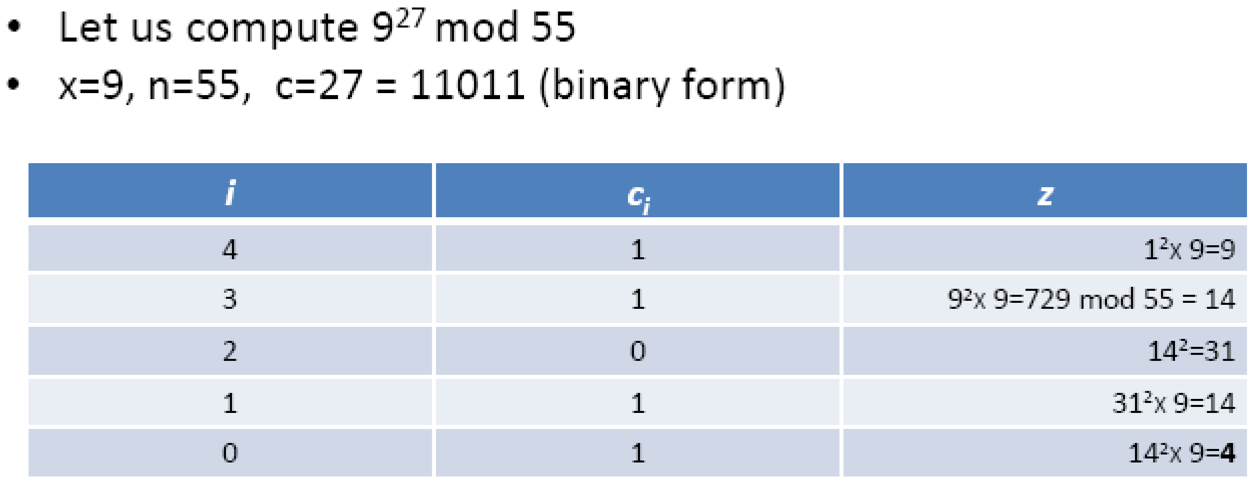
Gcd(3,40)=1, e=3 is a valid choice (note that 3 is a prime number)

Alice private exponent d: de=1 mod Φ(n), hence 3d=1 mod 40

d=27 since 3*27=81 = 1 mod 40

You send: **C** = M^e mod n = 4^3 mod 55 = 64 mod 55 = **9**

Alice receives C and computes C^d mod n = 9^{27}mod 55=4



- Let us compute 9^{27} mod 55
- x=9, n=55, c=27 = 11011 (binary form)

i	c_i	*z*
4	1	1^2x 9=9
3	1	9^2x 9=729 mod 55 = 14
2	0	14^2=31
1	1	31^2x 9=14
0	1	14^2x 9=**4**