Chapter 3
Password

Kind of passwords :

- **Password : (94** كلمة مرور مكونة من ارقام واحرف كبيرة وصغير ورموز)

this type of password contain A,a,1,@.....
Example : 12@Moh.?

- **Pin code :(10** كلمة مرور مكونة من ارقام فقط)

A string of numbers (0,1,2,3,4,5,6,7,8,9)

- **Pass phrase : (** كلمة مرور مكونة من أحرف عشوائية من جملة)

A sentence. I am studying cyber security in BZU
password : IamstyingcersecuinBU

- **Associative and cognitive passwords**

- **Pass face, pass image**

Password space:

-Pin code :

(0,1,2,3,4,5,6,7,8,9) 10 number of digits

For example : 6-digit PIN codes 10^6

- Password :

(number(10) , small letters(26) , capital letters(26) , special character(32)) : 94 number of digits

For example : 6-digit password 94^6

- Number of 6 letter combinations: 26^6
- Including capitals: 52^6
- Including numbers: 62^6
- All keyboard symbols: 94^6

At least 1 number:

All – wrong

Total number of 6-character passwords: 94^6

Number of 6-character passwords without numbers: 84^6

Answer: $94^6 - 84^6$

At least capital and 1 number ?

All – wrong one – wrong two + both wrong

- No restrictions: 94^6
- No capitals (94-26) = 68^6
- No numbers(94-10) = 84^6
- No capitals and no numbers (94-26-10)= 58^6

Answer : $94^6 - 68^6 - 84^6 + 58^6$

Q1 : At least capital and 1 special character ?

Have 4 different characters?

- First character: 94 possibilities
- Second character: (94-1) possibilities
- Third character: (94-2) possibilities
- Answer : 94 * 93 * 92 * 91

Q2: 6 different numbers for password content consisting of only upper and lower case letters?

Exactly 1 number?(6 digits)

Choose position where the number will be:
6 possibilities

Number on that position: 10 possibilities

All other 3 positions: (94-10) possibilities

Answer: $(6*10) * 84^5$

Trick: Place number first.

Q3: Exactly 1 capital ?(6 digits)

Exactly 1 number and exactly 1 capital?

Choose position for the number: 6 possibilities

Number on that position: 10 possibilities

Choose position for the capital: (6-1) possibilities

Capital on that position: 26 possibilities

All other 3 positions: (94-10 -26) possibilities

Answer: $(6*10) * (5*26) * 58^4$

Trick: Place number and capital first.

Q4 :Exactly 1 number and exactly 1 special character ?

Exactly 2 numbers?

n! / m! * (n-m)!

Choose 2 positions for the numbers : 6! / (2! * 4!) = 15 possibilities

Numbers on those position: 10 possibilities

All other 4 positions: (94-10) possibilities

Answer: $15 * 10^2 * 84^4$

Q5 : Exactly 3 numbers?

What is the probability that a random password of 6 characters has no number in it?

- **No restrictions:** 94^6

- **Number of 6-character passwords without numbers:** 84^6

Answer: $84^6 / 94^6 = 0{,}509$

القوانين:

- **At least one number :**
  All – wrong.

- **At least one number and one upper case :**
  All – wrong one – wrong two + wrong both

- **4 different characters :** (اول ما تشوف كلمة different اعرف انه تنازلي)
  if space =94
  94 * 93 * 92 * 91 *90

- **Exactly 1 number:**
  if space =94
  $(10*6) * 84^5$

- **Exactly 1 number and exactly 1 capital:**
  if space =94
  $(10*6) * (26*5) * 58^4$

- **Exactly 2 numbers:**
  $15 * 10^2 * 84^4$

Password Attacks

- Dictionary attack

Not fooled by(لا ينخدع بـ)

- Capitals

- Change of letters into numbers

- Permutations(التبديل بين الاحرف والارقام)

To not do list

الاشياء التي ينبغي عدم فعلها

PW which match a word (or reversed word) in a dictionary, regardless if some or all of the letters are capitalized

استخدام نفس الكلمة الموجودة في القاموس بغض النظر عما إذا كان البعض أو كل الحروف مكتوبة بأحرف كبيرة

PW based on user's account name

اعتماد كلمة المرور على اسم الحساب

PW which do not use mixed upper and lower case, or mixed letters and numbers, or mixed letters and punctuation

كلمات المرور التي لاتحتوي خليط من الارقام والاحرف العشوائية

PW based on user's account name

اعتماد كلمة المرور على اسم الحساب

PW which match a dictionary word with letters replaced by numbers (eg '3' for 'e')

استخدام كلمة مرور موجودة في القاموس مع تبديل الاحرف بأرقام

PW based on user's account name

اعتماد كلمة المرور على اسم الحساب

PW which match a dictionary word with letters replaced by numbers (eg '3' for 'e')

استخدام كلمة مرور موجودة في القاموس مع تبديل الحراف بأرقام

PW which are simple conjugations of a dictionary word (i.e. plurals, adding “ing” or “ed” to end of word, etc.)

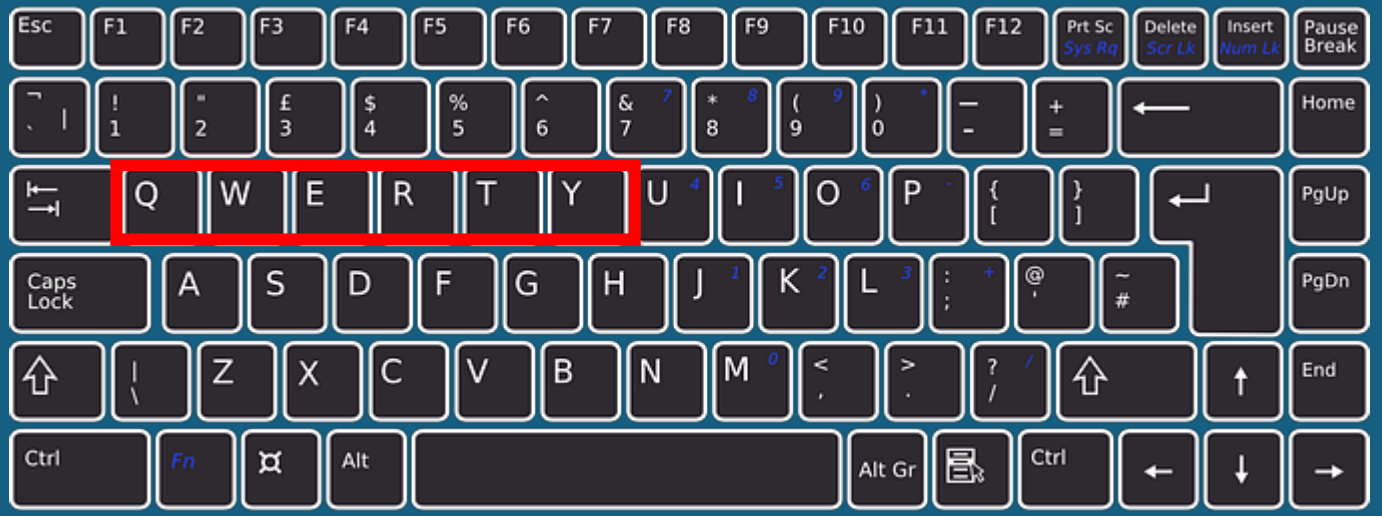
استخدام كلمة مرور موجودة في القاموس مع اضافة (ing – ed ……)

A password based on personal information such as name, phone number, and apartment number

كلمة مرور تعتمد على معلومات شخصية مثل الاسم و رقم الهاتف و رقم الشقة(ing – ed .....)

PW which are patterns from the keyboard (eg. “aaaaa” or “qwerty”)

كلمة مرور مكتوبة نفس ترتيب الكيبورد



Password: The PROBLEM!

We have limited memory:

- Can only remember 7±2 totally random symbols

Even more problems when:

- We have multiple passwords
- We need to change passwords regularly

What can we do

Pass phrase

Yesterday I watched a nice program on television.

Password : YIwanpot or Y1wanp0t

Use events on news or personal events when forced to change regularly

استخدام الأحداث في الأخبار أو الأحداث الشخصيةعندما تضطر إلى التغيير بانتظام

Encryption

- Shift every character fixed number of positions

- Shift every character by increasing number of positions