Recently, it was reported that 68 million DropBox user account details were leaked on the dark web by hacker.The data contains user mail addresses and hashed passwords, which use a kind of algorithm to encrypt the passwords. And then , the data dump was also verified by an security researcher on August 31.

In fact ,DropBox user infomation had been leaked in 2012.They found that hackers use their employee LinkedIn account to sign in their DropBox background management system and steal user data. But they didn't realized that how many user were affected by the hacker attack at that time until user acounts were leaked on the dark web.

Fortunately,Dropbox’s head said that user accounts have never been improperly accessed. The stolen passwords from Dropbox were encrypted by a hashing function called bcrypt.The hacker may not try to crack it due to the time and effort.But even without the passwords, the stolen email addresses can be quite useful for hackers to attack other affiliated Internet accounts so they inform their users to updae password, making them more strong and unique.

In my opinion, some security service and mechanism can be provided to mitigate to risk.Firstly ,additional login data can be used, such as a verification code send to a user cell phone.

Secondly, Increasing the level of data access permission is essential. Employees who don't have insufficient level can not access private data about user and company.

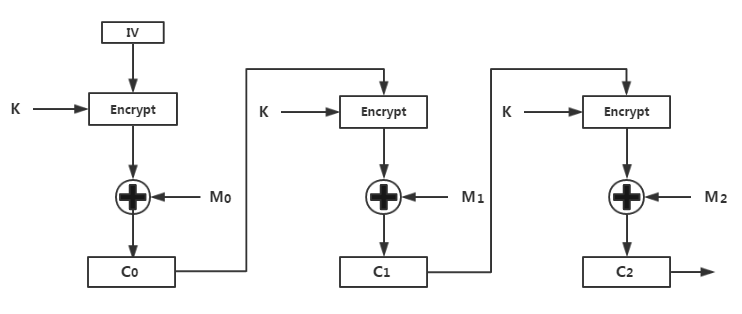
Thirdly, Companies can inroduce a security detection system to detect abnormal activity and illegal access behavior ,and also record such infomation to provide technicians to analyse them.

**Reference Link :**

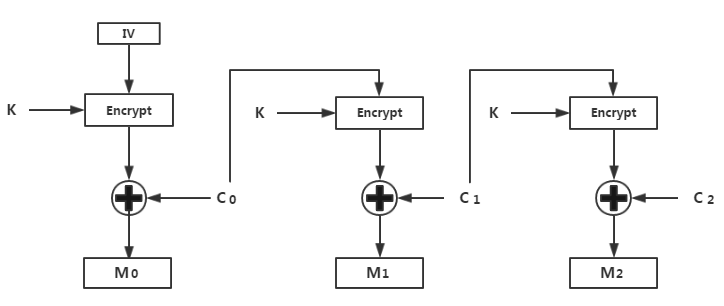
https://www.theguardian.com/technology/2016/aug/31/dropbox-hack-passwords-68m-data-breach

Mode1

Encrypt:

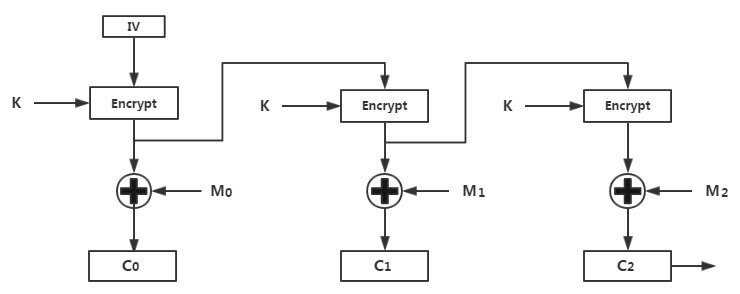


Decrypt:

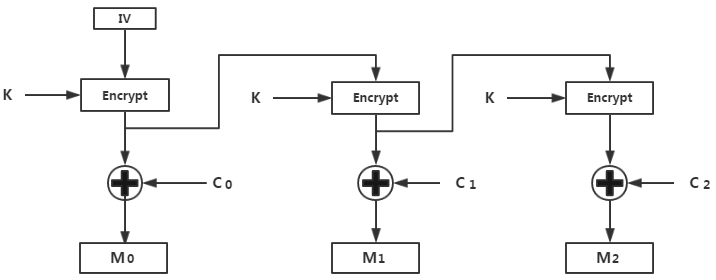


Mode2:

Encrypt:



Decrypt:



(b)Mode 2.M0 change,but M1 not, M1 is not related to C0

(c)Mode2

(d)Mode1 because decrypt : cipher can parral,but mode2 not wait the Enck()

**3. Number Theory**

X=54505818 Y=5818

### (a) Compute 41Y mod 18865 using the square-and-multiply method

41 5818 mod 18865=41 2+8+32+128+512+1024+4096 mod 18865

412=1681≡1681(mod 18865) √

414=(412) 2=2825761≡14876(mod 18865)

418=(414)2=221295376≡8926(mod 18865) √

4116=(418)2=79673476≡6581(mod 18865)

4132=(4116)2=43309561≡14386(mod 18865) √

4164=(4132)2=206956996≡7946(mod 18865)

41128=(4164)2=63138916≡16626(mod 18865) √

41256=(41128)2=276423876≡13896(mod 18865)

41512=(41256)2=193098816≡15541(mod 18865) √

411024=(41512)2＝241522681≡12951(mod 18865) √

412048=(411024)2=167728401≡8890(mod 18865)

414096=(412048)2=79032100≡6615(mod 18865) √

Hence 415818 mod 18865 = (1681×8926×14386×16626×15541×12951×6615) mod 18865 = 5676

(b) 1709 − X mod 23

(1709-54505818) mod 23=(1709 mod 23 - 54505818 mod 23) mod 23 = (7-4) mod 23=3

(c) gcd(54505818, 928374827)

Compute gcd(54505818, 928374827):

928374827=17×54505818+1775921

54505818=30×1775921+1228188

1775921=1×1228188+547733

1228188=2×547733+132722

547733=4×132722+16845

132722=7×16845+14807

16845=1×14807+2038

14807=7×2038+541

2038=3×541+415

541=1×415+126

415=3×126+37

126=3×37+15

37=2×15+7

15=7×2+1

2=2×1+0

**Hence gcd(54505818, 928374827)=1**

(d)Find x and z such that x · X + z · 928374827 = gcd(X,928374827)

Based on (c) :

1=15-7×2 =15 -2×(37-15×2)=5×15 - 2×37=5×(126-3×37)-2×37

=5×126-17×37=5×126-17×(415-3×126)=56×126 - 17×415

=56×(541-1×415)-17×415=56×541-73×415

=56×541-73×(2038-3×541)=275×541-73×2038

=275×(14807-7×2038)-73×2038=275×14807-1998×2038

=275×14807-1998×(16845-1×14807)=2273×14807-1998×16845

=2273×(132722-7×16845)-1998×16845=2273×132722+17909×16845=2273×132722+17909×(547733-4×132722)

=17909×547733-69363×132722=17909×547733-69363×(1228188-2×547733)=156635×547733-69363×1228188

=156635×(1775921-1×1228188) -69363×1228188

=156635×1775921-225998×1228188

=156635×1775921-225998×(54505818-30×1775921)

=6936575×1775921-225998×54505818

=(928374827-17×54505818)×1775921-225998×54505818

=1775921×928374827-30416655×54505818

Since ,x · 54505818 + z · 928374827 =1

Hence, x=-30416655, z=-30416655