IBM Security

הוראת סייבר: איך לחשוב; מה נורא; ודרך האתגר הטוב הרע והמכוער

אי כנס סייבר 15 ליולי 2016

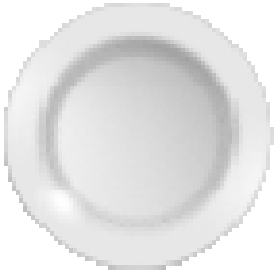
עודד מרגלית, מרכז המצוינות לאבטחת סייבר, יבמ באר שבע

IBM

המכוער: הקלות הבלתי נסבלת של התקפות סייבר

- **הנדסה חברתית**
  - www.youtube.com/watch?v=lc7scxvKQOo
  - www.darkre
    service/d/d-i
  - 5/28/2015 03
  - www.liveha
  - May 12, 201

המסוכן (נורא)



- **תפוס את הדגל**
  - **"דע את האויב"**
  - **חרב פיפיות**
  - **כייף!**
- **אבל**
  - **מסוכן!**
- **אז כיצד פותרים את הדילמה?**

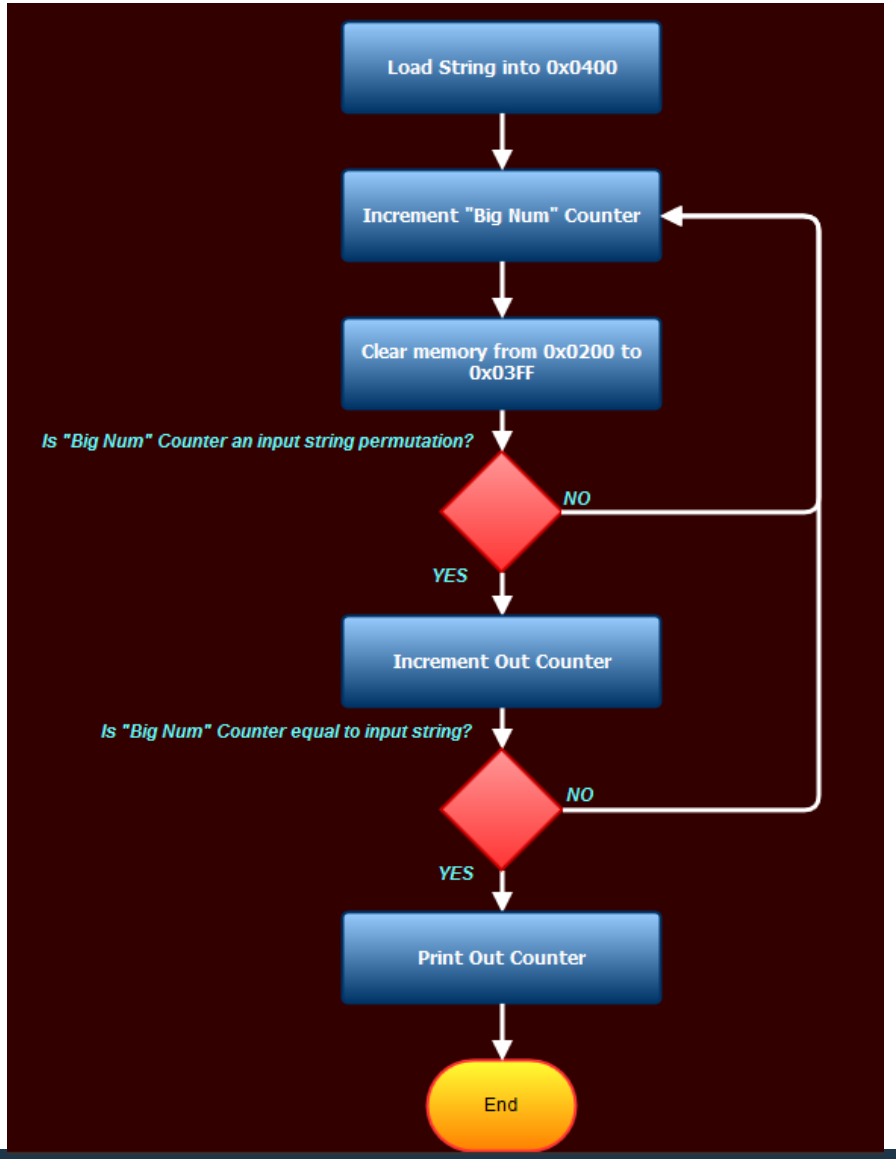
הטוב – חשוב מחוץ לקופסא

- **IEEEXtreme 2009**
  - #/bin/csh
    # Make sure we are using only the input digits and allowed operators
    tr -d '+\-*/()' < output | diff input –
    if ($? == 1) exit 1
    # Make sue no two digits are left without an operator between them
    grep '[0-9][0-9]' output
    if ($? == 0) exit 1
    # Once we passed the preconditions above, Score according to number of exercises solved correctly
    sed 's/$/-99.99999999/' output | bc -l | grep -c '^.00000‘
- How do you get to 100 from 5750004?

אתגרים לא פליליים

- **IEEEXtreme 2014**

```
BF 00 04 BE C0 00 56 31 C9 B4
00 CD 16 3C 2E AA E0 F7 F7 D1
29 D2 89 CD 5B 53 FE 07 75 03
43 EB F9 BF 00 02 89 F9 89 F8
F3 AA 89 FE AC 89 C3 FE 07 80
FB 2E 75 F6 FE 0F 5E 56 89 E9
AC 89 C3 FE 0F 7C D5 E2 F7 42
5E 56 89 E9 F3 A6 75 CA 5D 92
D4 0A E8 00 00 86 C4 04 30 CD
29 C3
```



מחומרה ועד אלגוריתמים מתמטיים

- **IEEEXtreme 2015**
  - `I=10*[]; B=50*[0];  M=256*[0]`

```
def f(I):
 B[49]=B[39];B[48]=B[38];B[47]=B[37];B[46]=B[36];B[45]=B[35];B[44]=B[34];B[43]=B[33];B[42]=B[32];B[41]=B[31];B[40]=B[30];
 B[39]=B[29];B[38]=B[28];B[37]=B[27];B[36]=B[26];B[35]=B[25];B[34]=B[24];B[33]=B[23];B[32]=B[22];B[31]=B[21];B[30]=B[20];
 B[29]=B[19];B[28]=B[18];B[27]=B[17];B[26]=B[16];B[25]=B[15];B[24]=B[14];B[23]=B[13];B[22]=B[12];B[21]=B[11];B[20]=B[10];
 B[19]=B[ 9];B[18]=B[ 8];B[17]=B[ 7];B[16]=B[ 6];B[15]=B[ 5];B[14]=B[ 4];B[13]=B[ 3];B[12]=B[ 2];B[11]=B[ 1];B[10]=B[ 0];
 B[ 9]=I[ 9];B[ 8]=I[ 8];B[ 7]=I[ 7];B[ 6]=I[ 6];B[ 5]=I[ 5];B[ 4]=I[ 4];B[ 3]=I[ 3];B[ 2]=I[ 2];B[ 1]=I[ 1];B[ 0]=I[ 0];
 x1=I[0]|I[1];x2=x1|I[2];x3=x2|I[3];x4=x3|I[4];x5=x4|I[5];x6=x5|I[6];x7=x6|I[7];x8=x7|I[8];x9=x8|I[9];
 y1=(not x9)|(I[0]&I[1]);y2=y1|(x1&I[2]);y3=y2|(x2&I[3]);y4=y3|(x3&I[4]);y5=y4|(x4&I[5]);y6=y5|(x5&I[6]);y7=y6|(x6&I[7]);y8=y7|(x7&I[8]);y9=y8|(x8&I[9]);
 c0=B[0]|B[10]|B[20]|B[30]|B[40];c1=B[1]|B[11]|B[21]|B[31]|B[41];c2=B[2]|B[12]|B[22]|B[32]|B[42];c3=B[3]|B[13]|B[23]|B[33]|B[43];
 c4=B[4]|B[14]|B[24]|B[34]|B[44];c5=B[5]|B[15]|B[25]|B[35]|B[45];c6=B[6]|B[16]|B[26]|B[36]|B[46];c7=B[7]|B[17]|B[27]|B[37]|B[47];
 c8=B[8]|B[18]|B[28]|B[38]|B[48];c9=B[9]|B[19]|B[29]|B[39]|B[49];c10=not (c0 | c1);c11=c0^c1;c12=c0&c1;
 c20=(c10&(not c2));c21=(c10&c2)|(c11&(not c2));c22=(c11&c2)|(c12&(not c2));c23=(c12&c2);
 c30=(c20&(not c3));c31=(c20&c3)|(c21&(not c3));c32=(c21&c3)|(c22&(not c3));c33=(c22&c3)|(c23&(not c3));c34=(c23&c3);
 c40=(c30&(not c4));c41=(c30&c4)|(c31&(not c4));c42=(c31&c4)|(c32&(not c4));c43=(c32&c4)|(c33&(not c4));c44=(c33&c4)|(c34&(not c4));c45=(c34&c4);
 c51=(c40&c5)|(c41&(not c5));c52=(c41&c5)|(c42&(not c5));c53=(c42&c5)|(c43&(not c5));c54=(c43&c5)|(c44&(not c5));c55=(c44&c5)|(c45&(not c5));
 c62=(c51&c6)|(c52&(not c6));c63=(c52&c6)|(c53&(not c6));c64=(c53&c6)|(c54&(not c6));c65=(c54&c6)|(c55&(not c6));
 c73=(c62&c7)|(c63&(not c7));c74=(c63&c7)|(c64&(not c7));c75=(c64&c7)|(c65&(not c7));
 c84=(c73&c8)|(c74&(not c8));c85=(c74&c8)|(c75&(not c8));
 c95=(c84&c9)|(c85&(not c9));
 e=(not c95)|y9;
 a=10*[0]
 a[0]=e|((((not c0)&(not c1)& (not c2)&(not c3)&(not c4))|(c0&c1&c2&c3&c4))^c0^c1^c2^c3^c4^(c3&(((c0^c8)&c1&c2&c4)^(((c0^c1)&c2&c5)^(c1&c4&c7))&c8)));
 a[1]=e|((((not c0)&(not c1)&(c2)&(not c5)&(c6))|(c0&c1&((not c2)&(not c6))&c5))^c0^c1^c2^c5^c6^(c4&((c0&c1&((c2&c3)^(c5&c6)))^(((c1&c7)^(c6&c9))&c3&c8))));
 a[2]=e|((((not c0)&(not c1)&(    c3)&(not c5)&(not c7))|(c0&c1&(not c3)&c5&c7))^c0^c1^c3^c5^c7^ (c0&c1&c2&(c3^c4)&c5)^((c3^c4)&c5&c7&c8&c9));
 a[3]=e|((c3&c5)^(c3&c6)^(c3&c8)^(c3&c9)^(c5&c6)^(c5&c8)^(c5&c9)^(c6&c8)^(c6&c9)^(c8|c9)^c3^c5^c6^c8^c9^(c0&c1&c3&c6&c9));
 a[4]=e|((c2&c5)^(c2&c7)^(c2&c8)^(c2&c9)^(c5&c7)^(c5&c8)^(c5&c9)^(c7&c8)^(c7|c9)^(c8&c9)^c2^c5^c7^(((c0&c5&c6)^(c1&c3&c4))&c7&c8));
 a[5]=e|((c0&c1)^c0^c2^c4^c6^c7^(c0&c1&c2&c3&c4)^(((c0&((c3&c5)^(c2&c4)))^(c1&c4&c6))&c7&c8)^(c3&c4&c6&((c2&c9)^(c5&c7))));
 a[6]=e|(c0^c1^c3^c4^c7^(c0&c1&c2&c4&c9)^(c0&((c1&c4)^(c3&c8))&c5&c7)^((((((c0^c1)&c5)^(c0&c4))&c2)^(c1&(c2^c7)&c4))&c6&c8));
 a[7]=e|(c2^c3^c4^(c0&((c2&c3)^((c2^c3)&c7))&c4&c8)^((((c0^c1)&c3&c5)^(((c0^c1)&(c4^c5))&c6))&c7&c8));
 M[sum([a[i]<<i for i in range(8)])]=1
output=int(input())
for i in range(output):
    f([ord(c)&1 for c in input()])
output = 1000*sum(M)-output
print(output)
```

לא צריך ללמד שפת סף (אסמבלי)

- **קיראו לי אמן חרבות מיושן**

אבל

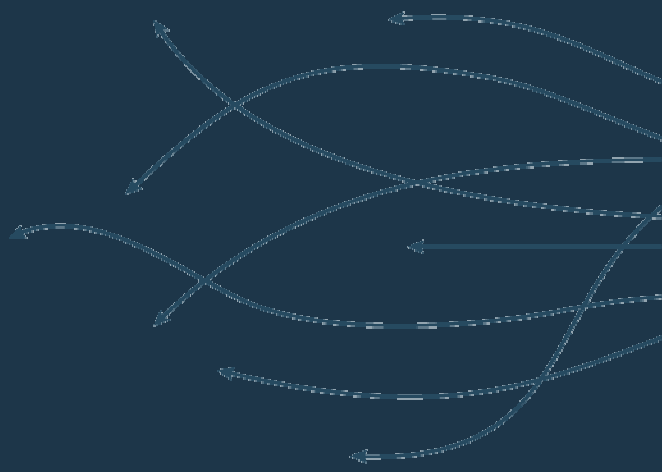
- **לדעתי זו אמנות לחימה נחוצה**
- **וזה גם כייף**

ואתגרים נוספים

- **פורום החידות של קודגורו**
  - codeguru.co.il/wp/?forum=%D7%97%D7%99%D7%93%D7%95%D7%AA
- **פינת החידות של יבמ**
  - research.ibm.com/ponder
- **אתרי אתגר תכנות**
  - www.hackerrank.com
- **תחרות תכנות**
  - www.ieee.org/xtreme

Codeguru xtreme
11.5
Aug 12th 2016

IBM Security



THANK YOU

FOLLOW US ON:

- ibm.com/security
- securityintelligence.com
- xforce.ibmcloud.com
- @ibmsecurity
- youtube/user/ibmsecuritysolutions

IBM