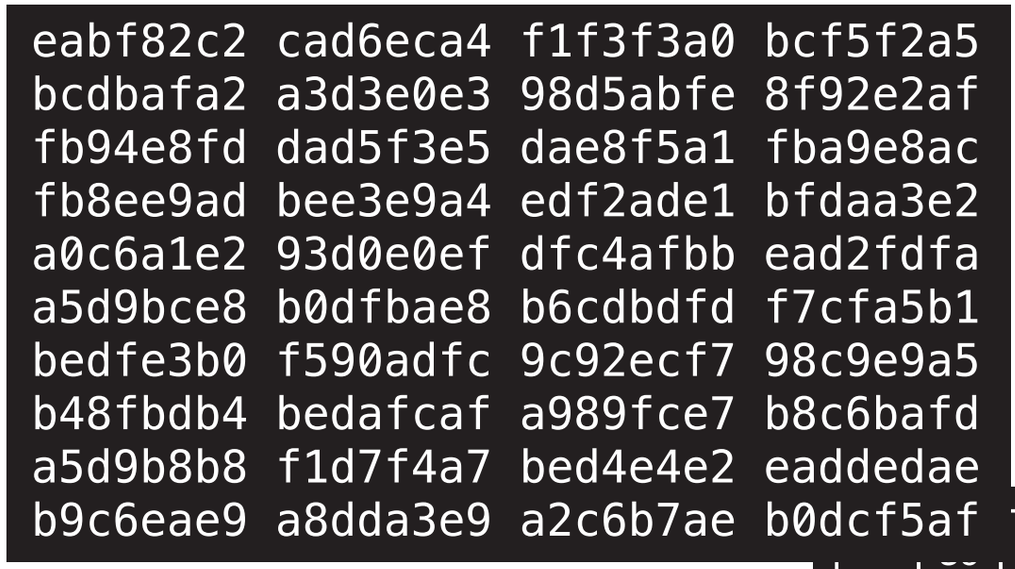
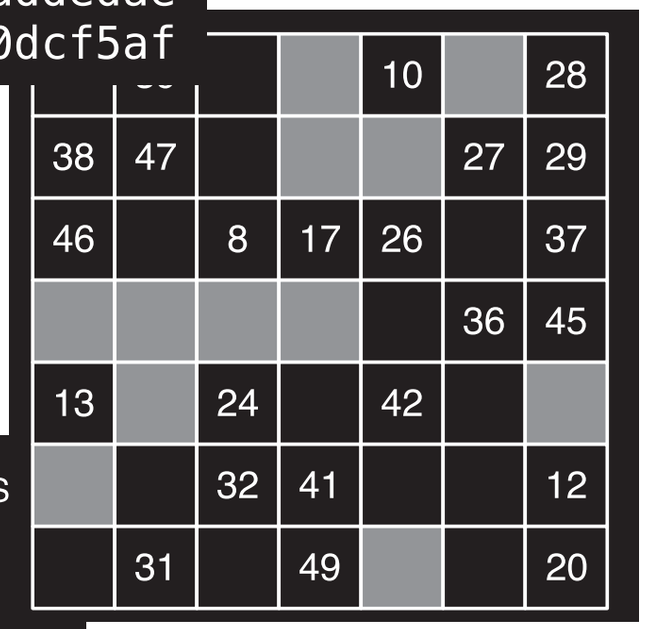
ShmooCon X Badge Contest

Darth Null

- Nine badges.
- Eight obvious stages.
- One final stage.
- One hidden stage.





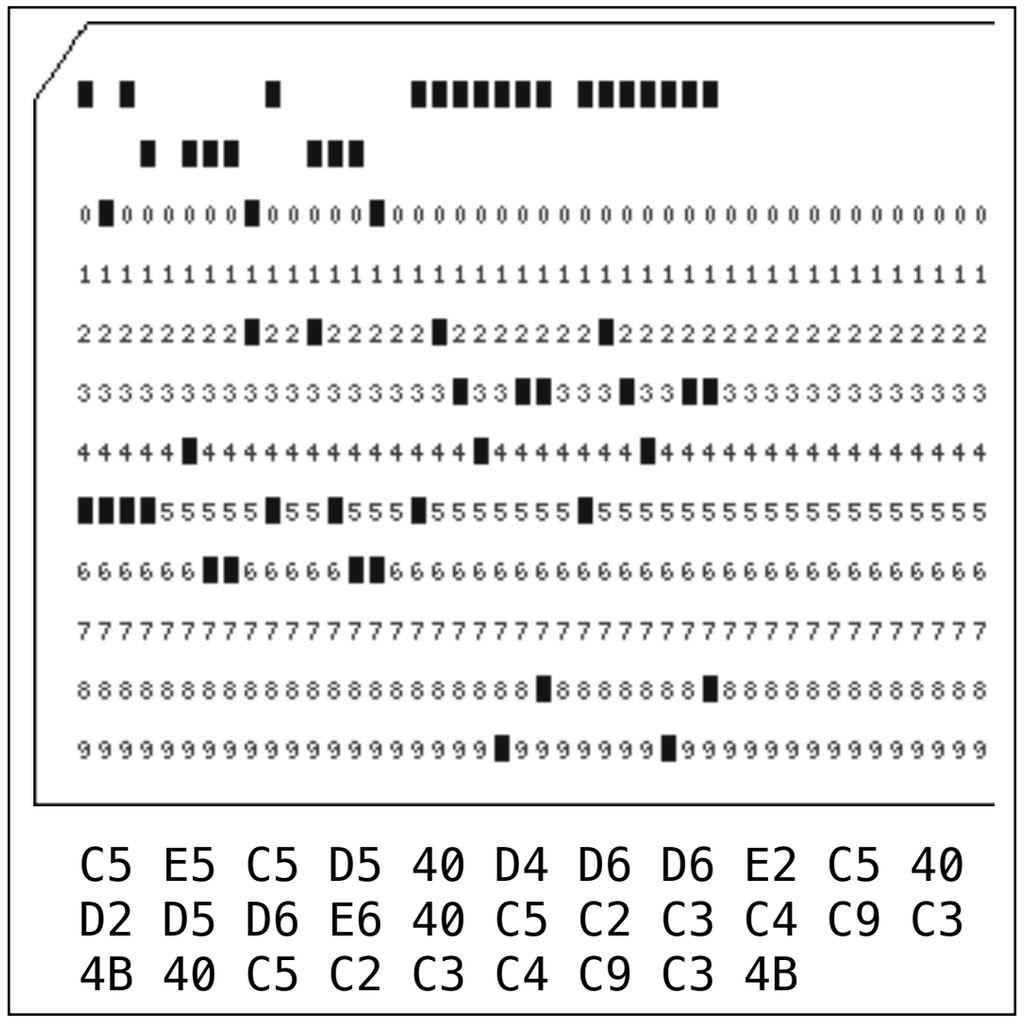
Put in the Right Order

- Will help with final stage
- Convenient reference for submitting answers
- Album of the Year Grammy Winners

Ray Charles	2005	Genius Loves Company
U2	2006	How to Dismantle an Atomic Bomb
Dixie Chicks	2007	Taking the Long Way
Herbie Hancock	2008	River: The Joni Letters
Robert Plant	2009	Raising Sand
Taylor Swift	2010	Fearless
Arcade Fire	2011	The Suburbs
Adele	2012	21
Mumford & Sons	2013	Babel

Stage 1 - “EBCDIC”

- One of G. Mark’s famous punched cards
- Hex at the bottom — but it’s not ASCII
- “EVEN MOOSE KNOW EBCDIC. EBCDIC.”
- Winner: Team Flowers By Irene



C5 E5 C5 D5 40 D4 D6 D6 E2 C5 40
D2 D5 D6 E6 40 C5 C2 C3 C4 C9 C3
4B 40 C5 C2 C3 C4 C9 C3 4B

Stage 2 - “Stego Games”

```
MATHISHARDBUTCRYPTOSFUNUSEMATHBREAKCRYPTOST
TLGJBPKZVATNRZWEOMPUCZEIHMGGTMJTETHQXBNGHHT
FBNATDVNEZQFCPPIJHNQDTVODATSMFOYURVUCDINRRQ
NCPUOGSPZZUTOKZAXPZNNRPZABZRNRZSHBDEDJAEDLZ
JPNVPYOOVOUTDHGYOLFZIPYAPHXKXHSLDYWRLOFTWST
RTFGIHFXRQHNCWLELWXXGLDANYADLRVLBOOPXWACHOM
JDVFCVWBWRYYPQYRFAUAYESFGWPCOGMGKDRAEZRFQHH
MYGQAQSMNUUBVXKCGHOKQEOFQHDRPWEDTZREJHDBDZZ
NJUFUKHWLKIOVSMNQHLMKPWXKYBYKQSPEBYMQSNSZJM
```

- Fun stego technique invented by G. Mark
- First line: MATH IS HARD BUT CRYPTOS FUN USE MATH BREAK CRYPTO ST
- Add all the lines together (M + T + F, etc.)
  - Z + A = 26 + 1= 27, 27 mod 26 = 1, A
- NOW TRY ADDING SQUARES PRIMES FIBONACCI NUMBERS ES

Relevant Solutions

```
1                   MATH IS HARD BUT CRYPTOS FUN USE MATH BREAK CRYPTO   ST
1 4 9               ONE IS KIND OF DEGENERATE CASE FOR SQUARE NUMBERS    EG
2 3 5 7             THE MOOSE THE MOOSE THE MOOSE IS ON THE LOOSE RUUUN  OG
1 1 2 3 5 8         WED NEVER USE FIBONACCI SEQUENCE IN A SHMOO GAMEE    AM
1 2 3 4 5 6 7 8 9   NOW TRY ADDING SQUARES PRIMES FIBONACCI NUMBERS      ES
```

- “STEGO GAMES” written in extra letters at end
- Winner: Team Flowers By Irene

Stage 3 - “Pseudobinary”

- A Magic Square
- Each row, column, and major diagonal adds to 175
- Shaded squares
  - Convert to letters, descramble
- Winner: Team Flowers By Irene

30	39	48	1	10	19	28
38	47	7	9	18	27	29
46	6	8	17	26	35	37
5	14	16	25	34	36	45
13	15	24	33	42	44	4
21	23	32	41	43	3	12
22	31	40	49	2	11	20

Stage 4 - “Chocolate Moose”

```
Axul axul axul!

Mkfrd T rz ikrryi mk zrlr morm
iurrm frqrum, brr noknkprmr zkkqr.

Ckuqm...dkxx mrlr brr noknkprmr.

Yxxz dxxz xxko, brr noknkprmr.
Wkxxu tm ty.

Kyf yxx irm brr zkkqr!

Orur, zkkqr, zkkqr, zkkqr!

Dxxz dxxz NOXNXPSMR ZXXQR.

Kyf yxx wxxm brr noknkprmr
  --  xxy brr zkkqr!
```

```
Bork bork bork!

Tudey I em gueeng tu meke thet
greet desert, zee chuculete muuse.

Furst...yuoo teke zee chuculete.

Yoom yoom oouh, zee chuculete.
Puoor it in.

Und noo get zee muuse!

Here, muuse, muuse, muuse!

Yoom yoom CHOCOLATE MOOSE.

Und noo poot zee chuculete
  -- oon zee muuse!
```

- Winner: Team Flowers By Irene

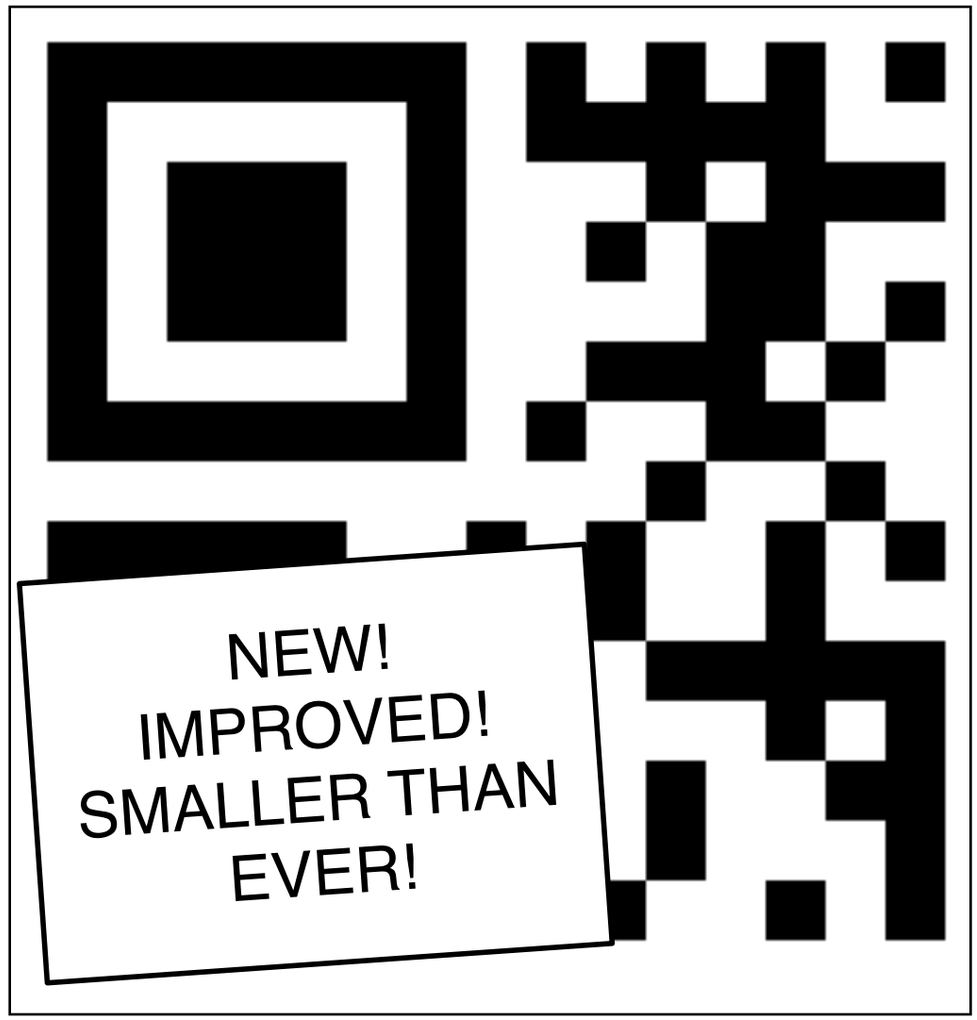
Stage 5 - “To Eleven”

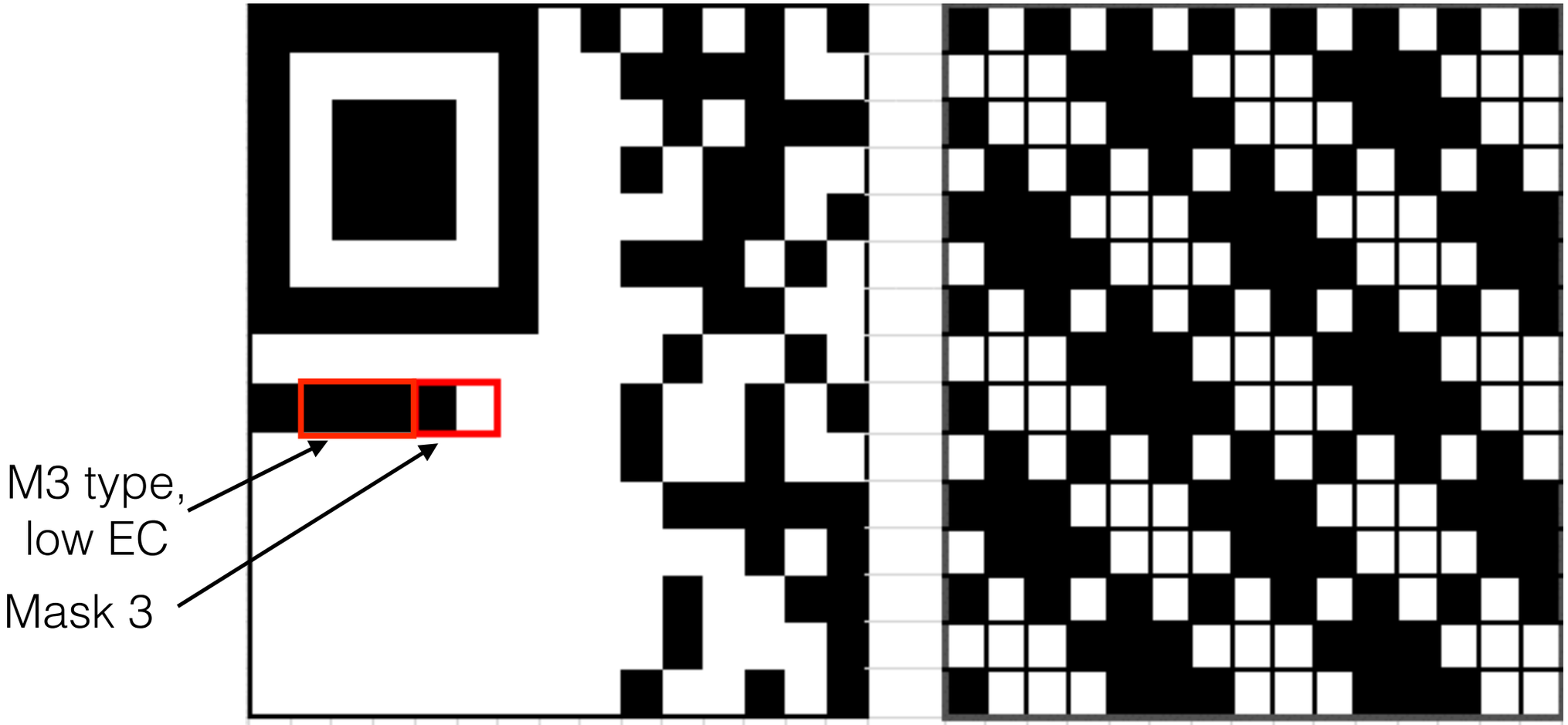
```
 copyriGht - In Europe, most music from before 1955 no longer
              covered by this
   BRitney - Received her first Grammy
pink floYd - Reunited for Live 8
     cReam - Legendary 60's band reunited at Royal Albert Hall
   rootkIt - Sony put this on music CDs
guitaRhero - First release of hugely popular music video game
   mAdonna - Tied Elvis' record for Top-10 singles
```

- GBRYRIRA -> ROT-13 -> “TO ELEVEN”
- Winner: Team Flowers By Irene

Stage 6 - “Fire Witch”

- Micro-QR code
- No iOS (or Android, AFAIK) apps
- Find the spec, decode manually
  - Need 2006 revision or newer
  - Read it carefully. :)
- Winner: Calvin & Hobbes





Code (left)
XOR
Mask (right)
gives bits
(bottom)

1	1	1	1	0	0	0	0	0	0	0	0	0	0	0
1	0	0	0	1	0	0	0	1	0	0	0	1	0	1
0	1	1	1	1	0	0	0	1	0	0	0	1	0	1
	M3			3	**Mask number**									
Code				50	**Mask reference**									
Type														
			0	1	0	0	0	1	1	0	46	**F**		
			0	1	1	0	1	0	0	1	69	**i**		
			0	1	1	1	0	0	1	0	72	**r**		
			0	1	1	0	0	1	0	1	65	**e**		
			0	1	0	1	0	1	1	1	57	**W**		
			0	1	1	0	1	0	0	1	69	**i**		
			0	1	1	1	0	1	0	0	74	**t**		
			0	1	1	0	0	0	1	1	63	**c**		
			0	1	1	0	1	0	0	0	68	**h**		

											0			
											0	0	0	0	1	0	0
											0	0	0	1	0	1	1
											0	0	0	0	1	1	0
											0	0	0	1	0	1	0
											0	0	1	1	0	0	1
											0	0	1	1	0	0	1
											0	1	0	1	0	1	0
	1	1	1	1	0	0	0	0	1	1	1	0	0	1
											0	0	1	1	1	0
											0	1	1	0	0	0
											1	0	0	1	1	0
											0	0	0	1	1	0
											1	0	1	0	0	1
											1	1	1	0	0	1

← r

← i

← F

← Nine bytes

← Byte mode

Stage 7 - “Moosetrap”

- Packet dump - 3 ping packets
  - From: 0a000001 (10.0.0.1)
  - To: cd86ace6 (205.134.172.230)
- Reverse-lookup of target host:
  - moosetrap.shmoo.com

```
205.134.172.227  www1.shmoo.com
205.134.172.228  www2.shmoo.com
205.134.172.229  www3.shmoo.com
205.134.172.230  moosetrap.shmoo.com
205.134.172.231  www5.shmoo.com
```

```
4500 0054 97cd 0000 4001 0000 0a00 0001
cd86 ace6 0800 de7d 6c3b 0000 52ad e510
000d 8a78 0809 0a0b 0c0d 0e0f 1011 1213
1415 1617 1819 1a1b 1c1d 1e1f 2021 2223
2425 2627 2829 2a2b 2c2d 2e2f 3031 3233
3435 3637

4500 0054 ffb9 0000 4001 0000 0a00 0001
cd86 ace6 0800 db97 6c3b 0001 52ad e511
000d 8d5c 0809 0a0b 0c0d 0e0f 1011 1213
1415 1617 1819 1a1b 1c1d 1e1f 2021 2223
2425 2627 2829 2a2b 2c2d 2e2f 3031 3233
3435 3637

4500 0054 a22d 0000 4001 0000 0a00 0001
cd86 ace6 0800 d92d 6c3b 0002 52ad e512
000d 8fc4 0809 0a0b 0c0d 0e0f 1011 1213
1415 1617 1819 1a1b 1c1d 1e1f 2021 2223
2425 2627 2829 2a2b 2c2d 2e2f 3031 3233
3435 3637
```

- Winner: Team Flowers By Irene

Stage 8 - “Gunslinger”

```
KJLNL KGDJT LWLWM HLKGD
LPLVG DJGLS LFLHL RGDLL
LSLKL JGDLF LHMGL WMHMH
GDMJL NLKGD MJMKL VLJMG
LFGSG DLFLV LJGDM JLNLK
GDJMM KLVMH LSLPL VLMLK
MGGDL LLWLS LSLWM MLKLJ
GVDQJ NLPLS LKGSG DJMKK
JVKHJ SJPJV JMJKK GGVDQ
```

- “KMON” code - Android serialization
- 16 letters in use (DFGHJKLMNPQRSTVW)
- Works in pairs:
  - 1st letter almost always L (44x), sometimes G, J, or M (11-16x), rarely K or D (4x & 2x).
  - 2nd letter: Any of the 16 (but D and K most frequent)

It’s Just Hexadecimal!

- Map nibbles (0-15) to consonants (DFGHJKLMNPQRSTVW)

- 41 (“A”) == JF, KJ == 54 (“T”)

- “The Moose in Black fled across the tundra, and the Gunslinger followed. Hile, GUNSLINGER.”

- Winner: Team Flowers By Irene

Stage 9 - Final

```
eabf82c2 cad6eca4 f1f3f3a0 bcf5f2a5
bcdbafa2 a3d3e0e3 98d5abfe 8f92e2af
fb94e8fd dad5f3e5 dae8f5a1 fba9e8ac
fb8ee9ad bee3e9a4 edf2ade1 bfdaa3e2
a0c6a1e2 93d0e0ef dfc4afbb ead2fdfa
a5d9bce8 b0dfbae8 b6cdbdfd f7cfa5b1
bedfe3b0 f590adfc 9c92ecf7 98c9e9a5
b48fbdb4 bedafcaf a989fce7 b8c6bafd
a5d9b8b8 f1d7f4a7 bed4e4e2 eaddedae
b9c6eae9 a8dda3e9 a2c6b7ae b0dcf5af
```

- Can’t do this yet — you need a key!

Hidden Stage - “Excelsior”

- Lines through “random” letters in URL
- Last badge had two lines - line them all up
- Winner: Jonathan Tomek

Hidden Stage - Part 2

- Last parts of URL form a ciphertext
- Note last one is one letter short
  - Gives an even number of letters in ciphertext
  - Hint towards Playfair cipher
  - Key is “EXCELSIOR”

```
vawiliEqb
Xnsqkcili
sCalivmxi
mnbizaEkm
dLdsLhici
dhkqSSmmS
bcIdhkmqa
Ouilbmfid
hkpzRake
```

- “You’re almost there. All you need to build the key are eight letters, eight primes, and eight words.”

Building the Key

Stage Word	Prime	Letter
EBCDIC	2	B
STEGOGAMES	3	E
PSEUDOBINARY	5	D
CHOCOLATEMOOSE	7	A
TOELEVEN	11	E
FIREWITCH	13	E
MOOSETRAP	17	A
GUNSLINGER	19	E

Key = “BEDAEEAE”

- Good guess: XOR encryption
- But not quite

```
$ cat final.ct | xor.py --hex --keyhex bedaeeae | xxd

0000000: 5465 6c6c 740c 020a 4f29 1d0e 022f 1c0b  Tellt...O).../..
0000010: 0201 410c 1d09 0e4d 260f 4550 3148 0c01  ..A....M&.EP1H..
0000020: 454e 0653 640f 1d4b 6432 1b0f 4573 0602  EN.Sd..Kd2..Es..
0000030: 4554 0703 0039 070a 5328 434f 0100 4d4c  ET...9..S(CO..ML
0000040: 1e1c 4f4c 2d0a 0e41 611e 4115 5408 1354  ..OL-..Aa.A.T..T
0000050: 1b03 5246 0e05 5446 0817 5353 4915 4b1f  ..RF..TF..SSI.K.
0000060: 0005 0d1e 4b4a 4352 2248 0259 2613 070b  ....KJCR"H.Y&...
0000070: 0a55 531a 0000 1201 1753 1249 061c 5453  .US......S.I..TS
0000080: 1b03 5616 4f0d 1a09 000e 0a4c 5407 0300  ..V.O......LT...
0000090: 071c 0447 1607 4d47 1c1c 5900 0e06 1b01  ...G..MG..Y.....
00000a0: 0a                                       .
```

“PBC” in 4-byte Blocks

```
Cipher:  eabf82c2 cad6eca4 f1f3f3a0 bcf5f2a5 bcdbafa2
Key:     bedaeeae bedaeeae bedaeeae bedaeeae bedaeeae
XORed:   54656c6c 740c020a 4f291d0e 022f1c0b 0201410c

PBC:     00000000 54656c6c 20696e66 6f407368 6d6f6f63

in hex:  54656c6c 20696e66 6f407368 6d6f6f63 6f6e2e6f

Plain:   T e l l    i n f  o @ s h  m o o c  o n . o
```

- Plaintext-block Chaining (not a “normal” mode, but…fun…)
  - (Cipher-block Chaining (CBC) had too obvious a pattern)
- XOR block N with plaintext from block N-1
- IV = 00 00 00 00

Final Stage Answer

Tell info@shmoocon.org

"There is no Dark Side of the Moose, really.
As a matter of fact it's all dark."

If you're the first to solve all of the stages,
you win!

- Winner: ....

Team Flowers By Irene

Winners!

- Stage 1 - Punch Card: Team Flowers By Irene
- Stage 2- Stego: Team Flowers By Irene
- Stage 3 - Magic Square: Team Flowers By Irene
- Stage 4 - Substitution: Team Flowers By Irene
- Stage 5 - Word Jumble: Team Flowers By Irene
- Stage 6 - Micro QR: Calvin & Hobbes
- Stage 7 - Ping Packets: Team Flowers By Irene
- Stage 8 - KMON Code: Team Flowers By Irene
- Hidden stage - Grille + Playfair: Jonathan Tomek
- Final stage - PBC XOR: Team Flowers By Irene