



Tales from the Crypto

G. Mark Hardy, CISM, CISA, CISSP
National Security Corporation
gmhardy@nationalsecurity.com
+1 410.933.9333
@g_mark



Which Would You Like to Hear?

- **Stories you can look up in the library?**
- **Ways you can win crypto contests?**

DEFCON XVIII



Stories I Can Tell You (over a beer... 😊)

- **Life or death by crypto**
- **Military crypto**
 - **Military use before WWII**
 - **Military ciphers of WWII**
 - **American ciphers**
 - **Japanese ciphers**
 - **German ciphers**
- **Commercial crypto**
 - **Early days of crypto**
 - **Banking security**
 - **eCommerce**

DEFCON XVIII



Some Basics: Types of Ciphers

- **Transposition ciphers**
 - Also known as permutation ciphers
- **Substitution ciphers**
 - Stream ciphers
 - Block ciphers
- **Product and exponentiation ciphers**
 - (advanced; won't cover here)

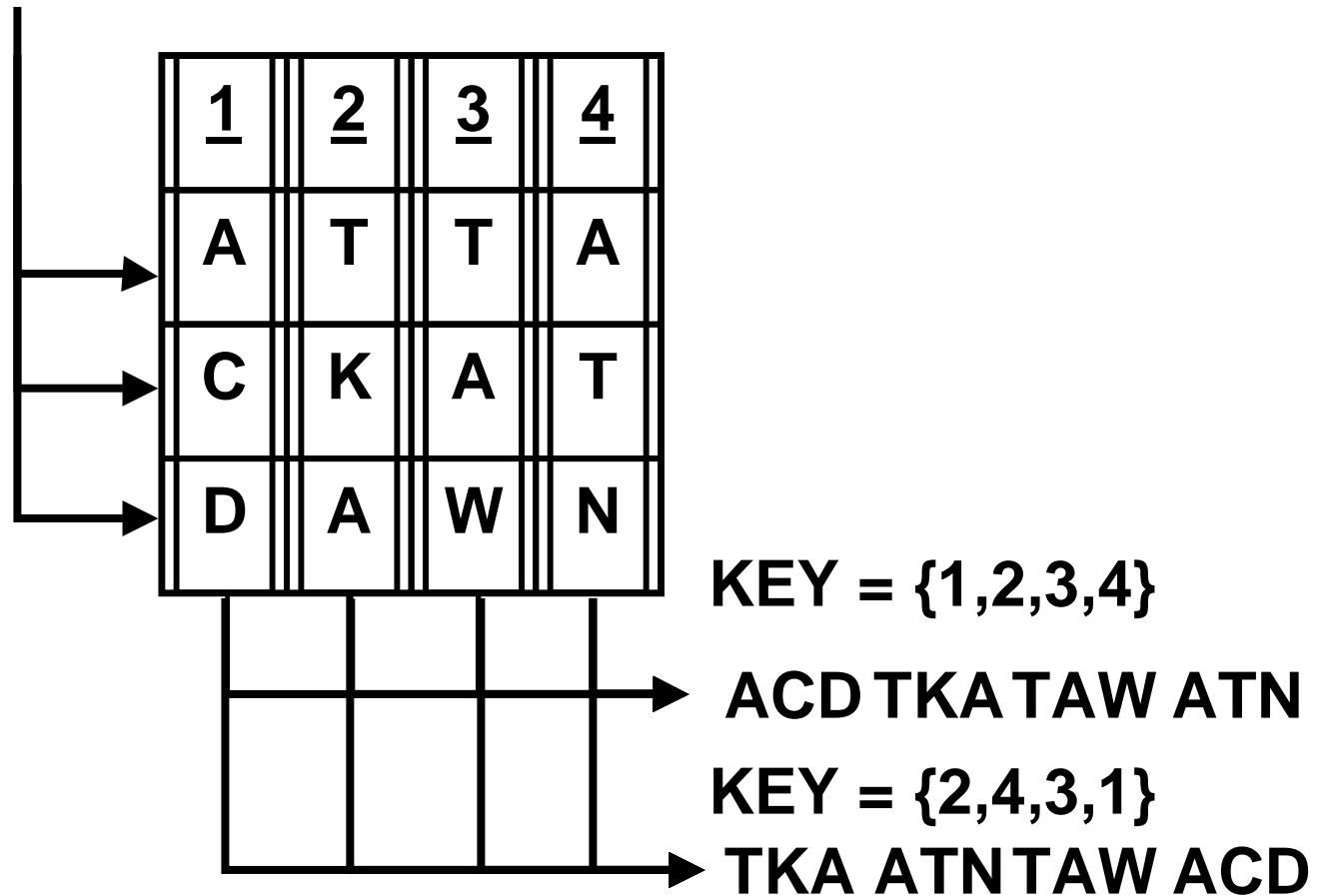
DEFCON XVIII



Transposition Ciphers

ATTACK AT DAWN

DEFCON XVIII





Substitution Cipher – Vigenère Cipher

DEFCON XVIII

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z



Substitution Cipher – Vigenère Cipher

ATTACK AT DAWN TOMORROW

DEFCON XVIII

ATTAC	KATDA	WNTOM	ORROW
PARTY	PARTY	PARTY	PARTY
	↓		
QULUB	ABLXZ	MOLIL	ESJIV



Substitution Cipher – Puzzle

DEFCON XVIII

SEND
+ MORE

MONEY



Substitution Cipher – Puzzle

DEFCON XVIII

$$\begin{array}{r} 9567 \\ + 1085 \\ \hline 10652 \end{array}$$

1. $S + M = MO$, so $M = 1$
2. $S + 1 = 10$, so $O = 0$
3. $S + 1 = 10$, so $S = 9$
4. $N + R = 1E$, $E + 1 = N$, so $R = 8$
5. Since $E+1 = N$, and $N + 8 > 11$,
E can be 3, 4, or 5.
6. If $E=3$ or 4, reach dead end; thus
 $E=5$
7. If $E=5$, then $N=6$
8. Only remaining values are $D=7$, $Y=2$



Playfair Cipher

- Playfair cipher (what I call the “don’t cheat” cipher): 3 simple rules
 - key “Hacker Jeopardy needs more crypto” (HACKERJOPDYNSTMTBFGILQUVWXZ)

DEFCON XVIII

A	B	C	D	E
F	G	H	I	J
K	L	M	N	O
P	R	S	T	U
V	W	X	Y	Z



H	A	C	K	E
R	J	O	P	D
Y	N	S	M	T
B	F	G	I	L
U	V	W	X	Z



Playfair Cipher

- **Encrypt**

- Now is the time for all
- NO WI ST HE TI ME FO RA LL
- NO WI ST HE TI ME FO RA LX LX
- SJ XG MY AH ML TK GJ JH IZ IZ

DEFCON XVIII

H	A	C	K	E
R	J	O	P	D
Y	N	S	M	T
B	F	G	I	L
U	V	W	X	Z



Substitution Cipher – Vernam Cipher or One-Time Pad

DEFCON XVIII

- $0 \oplus 0 = 0$

- $0 \oplus 1 = 1$

- $1 \oplus 0 = 1$

- $1 \oplus 1 = 0$

- $0 \neq 0 = 0$

- $0 \neq 1 = 1$

- $1 \neq 0 = 1$

- $1 \neq 1 = 0$

$$\begin{array}{r} 01101101101101 \\ \oplus 1010011011001011 \\ \hline 1100101101100110 \end{array}$$



If You Want to Win Crypto Contests

- You have to think like the guy (or girl) who develops them

DEFCON XVIII



BENEFACTOR

:? :

VN DB:GW TN

ZQ FM:DL YD

RD OC:RV UL

BO NB:JF RK

CB OV:JI LT

MA NM:IM TU

VR MT:ID BP

ED FM:FE YA

CN AT:WG JM



SHMOOCON 2008

- Okay, it was just after Mardi Gras
- My wife came home with 50 lbs. of beads
- I didn't want them kicking around the house for the next 10 years
- So, I did what any normal person would do...
- I created a SHMOOCON crypto contest
 - Using the beads, of course. :)

DEFCON XVIII



I Also Have Friends With Too Much Free Time...

DEFCON XVIII



**Im in yur b33dz,
breakin yur cipherz**





SHMOOCON 2008

- So, I placed the following randomly in registration packets:
 - 63 purple bead strings
 - 66 gold bead strings
 - 69 green bead strings
 - 30 pink bead strings
- L0st, Mouse, K, and G Mark wore red bead strings
 - And carried extra strings of red beads
 - Thus, anyone wearing red knew the solution
 - But those who were competing might not help others...
- We placed copies of the following messages in other packets:

DEFCON XVIII



Round 1

- **Plaintext**

- Congratulations on your opportunity to join our first Shmooscon crypto conundrum
- Your first task is to find participants with strings of Mardi Gras colors only
- Warning to you do not show up with anything pink or you disqualify instantly
- Bring your strings to a man or woman who has a string that is a color of blood
- And you will obtain an important hint that will assist in solving a first round

- **Notice anything unusual? :)**

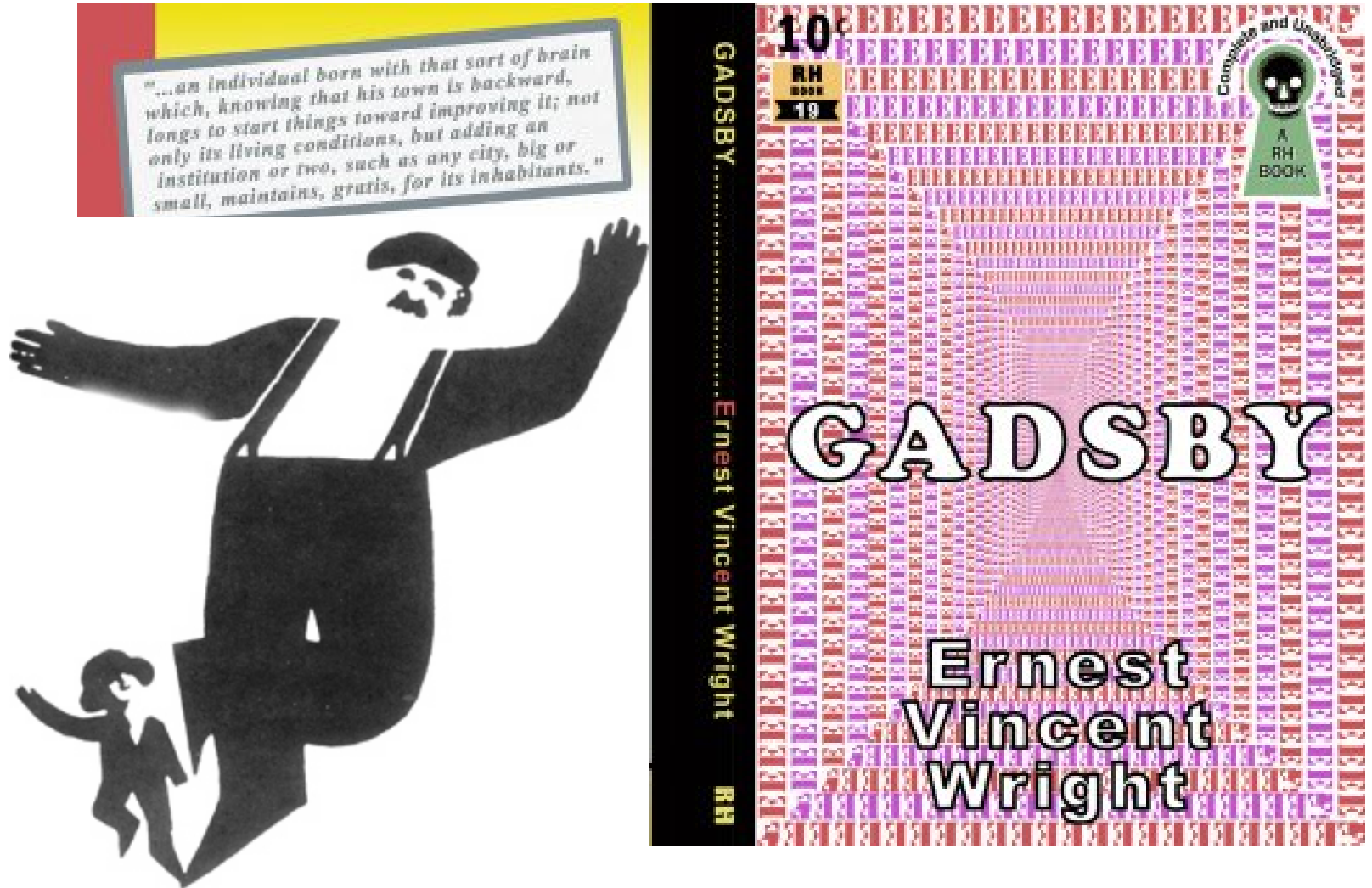
DEFCON XVIII



A Lipogram – like Gadsby

A Story of Over 50,000 Words
Without Using the Letter “E”

DEFCON XVIII





Round 1

DEFCON XVIII

- Padded plaintext
 - CONGRATULATIONSZONYOURZOPPORTUNITYZTOZJOINZO
URZFIRSTZSHMOOCONZCRYPTOZCONUNDRUMZ
 - YOURZFIRSTZTASKZISZTOZFINDZPARTICIPANTSZWITHZSTR
INGSZOFZMARDIZGRASZCOLORSZONLYZZ
 - AZWARNINGZTOZYOUZDOZNOTZSHOWZUPZWITHZANYTHIN
GZPINKZORZYOUZDISQUALIFYZINSTANTLYZZ
 - BRINGZYOURZSTRINGSZTOZAZMANZORZWOMANZWHOZHA
SZAZSTRINGZTHATZISZAZCOLORZOFZBLOODZZ
 - ANDZYOUZWILLZOBTAINZANZIMPORTANTZHINTZTHATZWIL
LZASSISTZINZSOLVINGZAZFIRSTZROUNDZ
- (Note the use of “Z”s for spaces and padding at end)
- So, using five Caesar ciphers, the offset of which is 7-
13-1-18-11:



Round 1

- Ciphertext

- JVUNYHABSHAPVUZGVUGFVBYGVWWVYABUPAFGAVGQVP
UGVBYGMPYZAGZOTVVJVUGJYFWAVGJVUBUKYBTG
- LBHEMSVEFGMGNFVMFMGBMSVAQMCNEGVPVCNAGFMJV
GUMFGEVATFMBSMZNEQVMTENFMPBYBEFMBAYLMM
- BAXBSOJOHAUPAZPVAEPAOPUATIPXAVQAXJUIABOZUIJOH
AQJOLAPSAZPVAEJTRVBMJGZAJOTUBOUMZAA
- TJAFYRQGMJRKLJAFYKRLGRSRESFRGJROGESFROZGRZS
KRSRKLJAFYRLZSLRAKRSRUGDGJRGXRTDGGVRR
- LYOKJZFKHTWWKZMELTYKLYKTXAZCELYEKSTYEKESLEKH
TWWKLDDTDEKTYKDZWGTYRKLKQTCDEKCFYOK

DEFCON XVIII



Round 1.5

DEFCON XVIII

Ready for more?

E more more more more?

A short visit to see

VISIT CC

A Hacker Looks Past 50

1, 2, 3, ...48,

49, 50 h4xor 

A painless operation

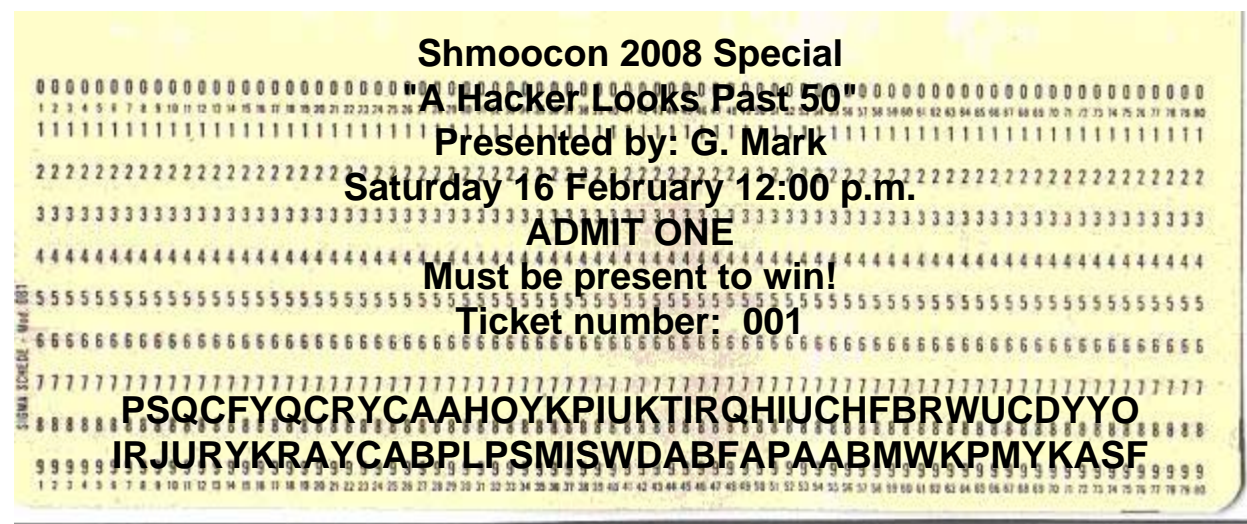
= a o_er_t_o_.



Round 2

DEFCON XVIII

- Round 2 was G Mark's talk "A Hacker Looks Past 50" (a sequel to previous talk "A Hacker Looks At 50")
- Handed out punched card with messages encrypted at the bottom





Round 2

- Playfair cipher (what I call the “don’t cheat” cipher)
 - key "A Hacker Looks Past Fifty"
(AHCKERLOSPTFIYBDGJMNQUVWYZ)

A	B	C	D	E
F	G	H	I	J
K	L	M	N	O
P	Q	R	S	T
U	V	W	X	Y



A	H	C	K	E
R	L	O	S	P
T	F	I	Y	B
D	G	J	M	N
Q	U	V	W	Y

DEFCON XVIII



Round 2 Messages

DEFCON XVIII

- GO AHEAD EMAIL MARDIGRAS AT SHMOOCON DOT INFO FOR THE FIRST OF FOUR PIECES OF THE ROUND TWO PUZZLE
- OH TRY TO FIND WWW DOT SHMOOCON DOT INFO SLASH BEADSECRET FOR SECONDARY PUZZLE PIECE KEEP GOING
- FOR FUN DIAL THE ALOHA STATE NINE FIVE FOUR NINE TWO DOUBLE THREE FOR THE THIRD IMPORTANT MESSAGE
- SOMETIMES THE EASIEST WAY TO GET WHAT YOU WANT IS TO JUST ASK THE PERSON YOU MET THREE TIMES NICELY



Round 2 Messages Padded for Encryption

DEFCON XVIII

- GOAHEADEMAILMARDIGRASATSHMOXOCON
DOTINFOFORTHEFIRSTOFFFOURPIECESOFTH
EROUNDTWOPUZZL
- OHTRYTOFINDWWXWDOTSHMOOCONDOTINF
OSLASHBEADSECRETFORSECONDARYPUZX
ZLEPIECEKEEPGOIN
- FORFUNDIALTHEALOHASTATENINEFIVEFOU
RNINETWODOUBLETHREEFORTHETHIRDIMP
ORTANTMESSAGE
- SOMETIMESTHEEASIESTWAYTOGETWHATYO
UWANTISTOJUSTASKTHEPERSONYOU METTH
REETIMESNICELY



Round 2 Messages Encrypted With Playfair Cipher

MLHCAHQADCFODCTUFMTIRRKYRCGSWIOSMMRFYGYLI
SLFAHBATORYLILATOBARKKPLIFAAPRWQGIUSRVUVP

Can't have double letters in Playfair in odd-even index positions

LCDTBFLIYMMUXZUMRILKWI IOSMMRFYGYSPRHLKQP
RUPKAOABILLPAKSMURSTRZUZVPPBBCKAEAPBMLYM

ILLTXDMTHRFAAHOSCHRYRDKQYMHBFWHBRWSDYMA
B CIMRZTPHFAPAHSLSFAABCFTUMWRSTDKDIDKPRKQH

PSQCFYQCRYCAAHOYKPIUKTIRQHIUCHFBRWUCDY
YO IRJURYKRAYCABPLPSMISWDABFAPAABMWKPMYKASF

DEFCON XVIII



So if you do each task, you get...

Autoresponder from
mardigras@shmoocon.info:

This is the first clue.

T A W S A G K G M I E 5 4

Send another e-mail to the same domain
using the numbers you find in the clues
If you get them all (and in the right order)
The fourth hint will be given to you.

[http://www.gmarkhardy.com/
shmoocon/beadsecret/clue2.txt](http://www.gmarkhardy.com/shmoocon/beadsecret/clue2.txt)

My hat's off to you!
You've solved puzzle two.
So here is some more
information to chew:

H G O T Y M A I E T A 7 2

Hurry, hurry, don't delay
You must solve the rest
By the close of the day

Third clue provided as a voice mail
message from (808) 954-9233:

E I R O T A R V W E D 1 8

Fourth clue (told to send e-mail to
571428@shmoocon.info):

Here is the fourth piece of four
So you need look no more:

M C D S O R E E H B S

Did you find this with ease?
Or use the force of a brute?
Either way, solve the puzzle
And collect your loot.

DEFCON XVIII



Four Clues

- Clues 1-4; transpose vertical to horizontal:

- T A W S A G K G M I E 5 4

- H G O T Y M A I E T A 7 2

- E I R O T A R V W E D 1 8

- M C D S O R E E H B S

- And you get:

- THE MAGIC WORDS TO SAY TO GMARK ARE
GIVE ME WHITE BEADS 571428

DEFCON XVIII



Crypto Can Pay Off

- I bought each of them a round-trip ticket to DEFCON that year.
 - Then they spent their time trying to solve L0st's puzzle instead of mine
 - Jolly texted me at closing ceremony, “any hints?”
 - I replied, “start saving your money for next year's plane ticket. :P”
- By the way, that 2008 DEFCON puzzle remains unsolved*...

DEFCON XVIII



DEFCON 2008

DEFCON XVIII

VFLASGGGGIUGAAGYBDAWHOEVHUUVLLHGJYOLGFGP
GHALGGGOAAGGJPLLHZKAGZSLRXHSRYHKFPVKISTF
XBMGRMBULEMPBMSRGMEMYRGMGRGHFMAGNMRLRZOM
GXMJRMLNBMEMUAZEGNQEQBGPSZRYZLDPYQDUGEPL
BVQZWOOBPPUSAZJEAUBTMATDFAJTTAUIFDSAQPVI
PFTIBOPWAUF OFHFAAJPASZSXMSBMFFMERIUSDZFU
QRJRWGDNMCZQTGYRZGFWRLRJRUF RSYWWKARAGMLS
RRGSKGMWYZKGSREOAVDKAQRZDTRKSDWWUYIVUSAQ
KCPNCEJPKPPAFFFZZKDKEPEPZZFXRCOKLAVDYDKO
XTXEJHKKPPEKECEMSKKWEDBLEEDBZDEDZKSGJAZOW



DEFCON XVIII

***ONE person has solved this
(and flew to DEFCON XVIII on my dime)**



DEFCON XVIII

You Can Create Your Own Crypto

**But be careful – it's like packing your
own parachute**

You have better be really GOOD!



SHMOOCON 2009

DEFCON XVIII












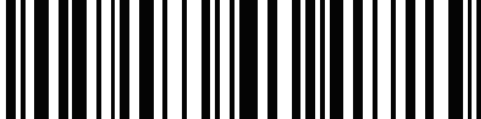


- What was THAT all about?
- Morse code
- Bar code



All Eight Badges

DEFCON XVIII

Left Border	Right Border	Bar Code
		
		
		
		
		
		
		
		



All Eight Badges

DEFCON XVIII

Left Border	Right Border	Bar Code
MOOSLETO	EHWXJBRG	111235813218
MOOSLEDE	FENSESXM	211235813215
CHOCOLAT	EMOOSEZA	311235813212
MOOSEKAT	EERSUCWR	411235813219
ROOMWITH	AMOOSEOK	511235813216
BEANONYM	OOSEEJYN	611235813213
MOOSEYFA	TEHZMEID	711235813210
MOOSENUG	GETEXBOT	811235813217



Table of Values

DEFCON XVIII

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	M	O	O	S	L	E	T	O	E	H	W	X	J	B	R	G
2	M	O	O	S	L	E	D	E	F	E	N	S	E	S	X	M
3	C	H	O	C	O	L	A	T	E	M	O	O	S	E	Z	A
4	M	O	O	S	E	K	A	T	E	E	R	S	U	C	W	R
5	R	O	O	M	W	I	T	H	A	M	O	O	S	E	O	K
6	B	E	A	N	O	N	Y	M	O	O	S	E	E	J	Y	N
7	M	O	O	S	E	Y	F	A	T	E	H	Z	M	E	I	D
8	M	O	O	S	E	N	U	G	G	E	T	E	X	B	O	T



What's Left Over?

DEFCON XVIII

- **Telomeres**

- H W X J B R S X Z U C W O E J Y N H Z M E I
D E X B O T

- **Can you see anything left-to-right?**

- H W X J B R S X Z U C W O E J Y N H Z M E I
D E X B O T

- BRUCE HEIDE [sic] XO

- **What's left?**

- H W X J S X Z W O J Y N Z M B T

- How many? Could that be significant?



Table of Values

DEFCON XVIII

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	M	O	O	S	L	E	T	O	E	H	W	X	J	B	R	G
2	M	O	O	S	L	E	D	E	F	E	N	S	E	S	X	M
3	C	H	O	C	O	L	A	T	E	M	O	O	S	E	Z	A
4	M	O	O	S	E	K	A	T	E	E	R	S	U	C	W	R
5	R	O	O	M	W	I	T	H	A	M	O	O	S	E	O	K
6	B	E	A	N	O	N	Y	M	O	O	S	E	E	J	Y	N
7	M	O	O	S	E	Y	F	A	T	E	H	Z	M	E	I	D
8	M	O	O	S	E	N	U	G	G	E	T	E	X	B	O	T



What About Those Bar Codes?

- **Common sequence**
 - [x]1123581321[y]
 - 1 – 1 – 2 – 3 – 5 – 8 – 13 – 21
 - **Fibonacci Series**
 - First eight terms
 - Eight badges
 - Eight indexes (or indices :)
 - **What to do with them?**
 - Think shift register

DEFCON XVIII



Table of Values

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	
1	1	M	O	O	S	L	E	T	O	E	H	W	X	J	B	R	G
1	2	M	O	O	S	L	E	D	E	F	E	N	S	E	S	X	M
2	3	C	H	O	C	O	L	A	T	E	M	O	O	S	E	Z	A
3	4	M	O	O	S	E	K	A	T	E	E	R	S	U	C	W	R
5	5	R	O	O	M	W	I	T	H	A	M	O	O	S	E	O	K
8	6	B	E	A	N	O	N	Y	M	O	O	S	E	E	J	Y	N
13	7	M	O	O	S	E	Y	F	A	T	E	H	Z	M	E	I	D
21	8	M	O	O	S	E	N	U	G	G	E	T	E	X	B	O	T



Table of Values

DEFCON XVIII

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	M	O	O	S	L	E	T	O	E	H	W	X	J	B	R	G
2	M	O	O	S	L	E	D	E	F	E	N	S	E	S	X	M
3	A	C	H	O	C	O	L	A	T	E	M	O	O	S	E	Z
4	W	R	M	O	O	S	E	K	A	T	E	E	R	S	U	C
5	S	E	O	K	R	O	O	M	W	I	T	H	A	M	O	O
6	O	S	E	E	J	Y	N	B	E	A	N	O	N	Y	M	O
7	E	Y	F	A	T	E	H	Z	M	E	I	D	M	O	O	S
8	X	B	O	T	M	O	O	S	E	N	U	G	G	E	T	E



Table of Numeric Equivalents

DEFCON XVIII

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	13	15	15	19	12	5	20	15	5	8	23	24	10	2	18	7
2	13	15	15	19	12	5	4	5	6	5	14	19	5	19	24	13
3	1	3	8	15	3	15	12	1	20	5	13	15	15	19	5	26
4	23	18	13	15	15	19	5	11	1	20	5	5	18	19	21	3
5	19	5	15	11	18	15	15	13	23	9	20	8	1	13	15	15
6	15	19	5	5	10	25	14	2	5	1	14	15	14	25	13	15
7	5	25	6	1	20	5	8	26	13	5	9	4	13	15	15	19
8	24	2	15	20	13	15	15	19	5	14	21	7	7	5	20	5



Table of Numeric Equivalents

DEFCON XVIII

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	
1	13	15	15	19	12	5	20	15	5	8	23	24	10	2	18	7	
2	13	15	15	19	12	5	4	5	6	5	14	19	5	19	24	13	
3	1	3	8	15	3	15	12	1	20	5	13	15	15	19	5	26	
4	23	18	13	15	15	19	5	11	1	20	5	5	18	19	21	3	
5	19	5	15	11	18	15	15	13	23	9	20	8	1	13	15	15	
6	15	19	5	5	10	25	14	2	5	1	14	15	14	25	13	15	
7	5	25	6	1	20	5	8	26	13	5	9	4	13	15	15	19	
8	24	2	15	20	13	15	15	19	5	14	21	7	7	5	20	5	
SUM	113	102	92	105	103	104	93	92	78	67	119	97	83	117	131	103	113
Mod26	9	24	14	1	25	0	15	14	0	15	15	19	5	13	1	25	9



Convert Back to Text

- (1=A, 2=B, ... 26=Z)

- 9 24 14 1 25 0 15 14 0
15 15 19 5 13 1 25
- I X N A Y O N
O O S E M A Y

DEFCON XVIII

*Congratulations. You have just discovered the secret message. Your patience has been rewarded.
Go to my website subdirectory reciprocal of this page number to six places.*



What Kind of Sick Mind Comes Up With This?

Ⓢ = ONLY ONE IN COLUMN,
SO MUST BE FIXED.
x = CAN VARY, BUT SOME MUST BE RIGHT
DRILLIN = 1
(Z = NULL)

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
1	M	O	O	S	L	E	T	O	E	Ⓢ	Ⓢ	Ⓢ	Ⓢ	B	R	G
2	M	O	O	S	L	E	D	E	F	E	N	S	E	Ⓢ	Ⓢ	M
3	Ⓢ	Ⓢ	C	H	O	C	O	L	A	T	E	M	O	O	S	E
4	Ⓢ	Ⓢ	M	O	O	S	E	K	A	T	E	E	R	S	U	C
5	S	E	Ⓢ	K	R	O	O	M	W	I	T	H	A	M	O	O
6	O	S	E	E	Ⓢ	Ⓢ	Ⓢ	B	E	A	N	O	N	Y	M	O
7	E	Y	F	A	T	E	H	Ⓢ	Ⓢ	Ⓢ	Ⓢ	Ⓢ	Ⓢ	Ⓢ	Ⓢ	Ⓢ
8	Ⓢ	Ⓢ	Ⓢ	Ⓢ	Ⓢ	Ⓢ	Ⓢ	Ⓢ	Ⓢ	Ⓢ	Ⓢ	Ⓢ	Ⓢ	Ⓢ	Ⓢ	Ⓢ
	I	X	N	A	Y	Z	O	N	Z	O	O	S	E	M	A	Y

12	B	E	A	N	O	N	Y	M	O	O	S	E				
15	A	N	O	N	Y	M	O	O	S	E						
12	M	O	O	S	E	K	A	T	E	E	R	S				
9	M	O	O	S	L	E	T	O	E							
13	M	O	O	S	L	E	D	E	F	E	N	S	E			
14	C	H	O	C	O	L	A	T	E	M	O	O	S	E		
14	R	O	O	M	W	I	T	H	A	M	O	O	S	E		
10	M	O	O	S	E	Y	F	A	T	E						
11	M	O	O	S	E	N	U	G	G	E	T					

M	O	O	S	L	E	T	O	E					B	R	G
M	O	O	S	L	E	D	E	F	E	N	S	E			M
C	H	O	C	O	L	A	T	E	M	O	O	S	E		A
M	O	O	S	E	K	A	T	E	E	R	S	U	C		R
R	O	O	M	W	I	T	H	A	M	O	O	S	E		K
B	E	A	N	O	N	Y	M	O	O	S	E				
M	O	O	S	E	Y	F	A	T	E	H					
M	O	O	S	E	N	U	G	G	E	T					

BARCODE
 1 1 2 3 5 8 1 3 2 1
 SIZE [1-8] CHECKSUM



The Same One That Came Up With This...

DEFCON XVIII

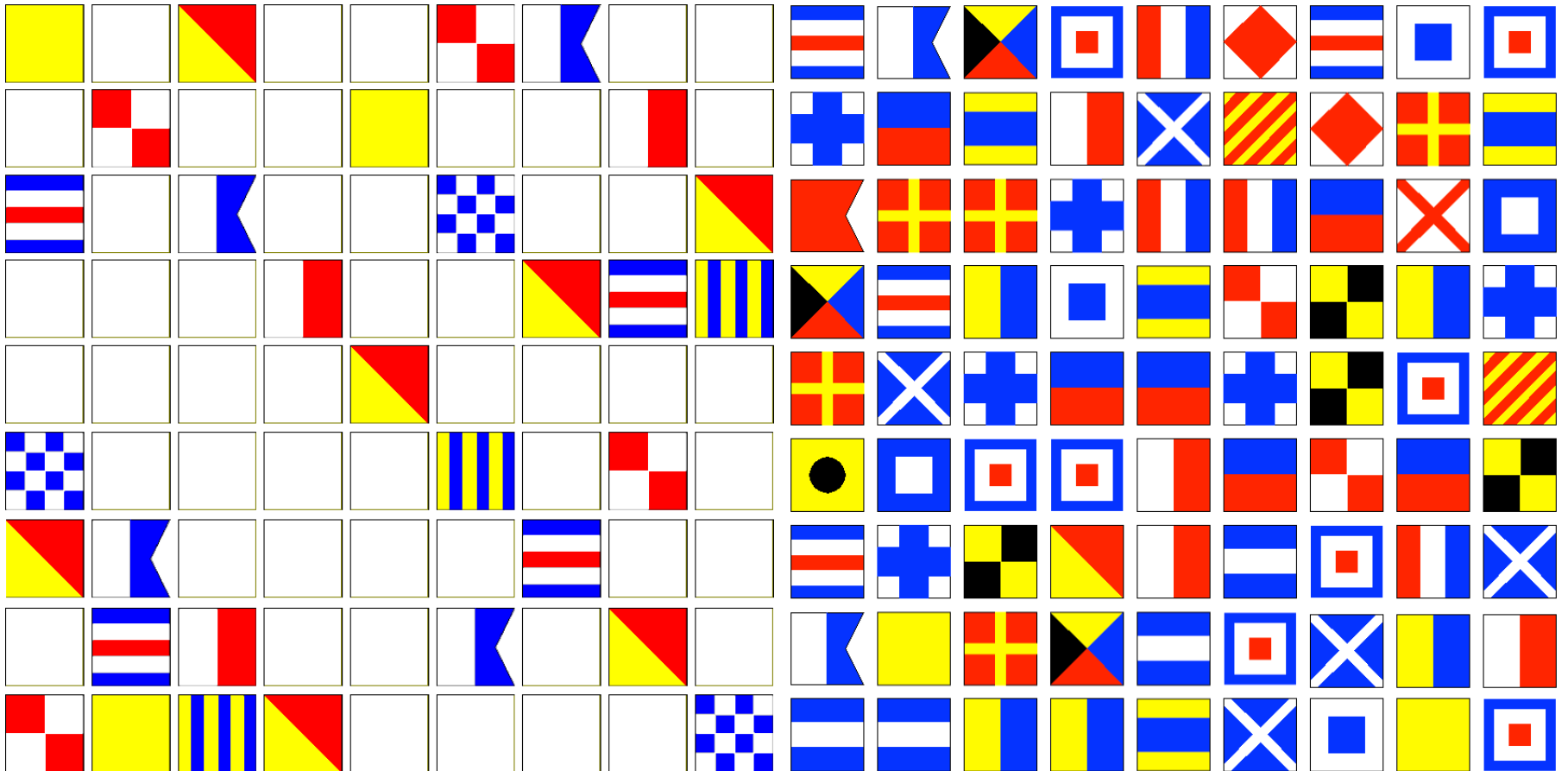
- **The DEFCON XVIII crypto contest**
 - Look for gold on the DC CD
- **Go have some fun!**
 - Follow me at @g_mark for clues



Other G. Mark Crypto Contests

QUAHOGCON 2010

DEFCON XVIII



Other G. Mark Crypto Contests SHMOOCON 2010



ERINW Living Security

Trustwave SpiderLabs

G2

22.612239 17.080442 345 3973

17.205642 -62.594003 114 5251

JOLINSON

JEFFERSON

REGISTRATION

EAST

SOUTH

NORTH

WEST

TRUMAN

TAYLOR

TRIMAN

ATRIVM

The good Marshal Ballroom



DEFCON XVIII

Tales from the Crypto

G. Mark Hardy, CISM, CISA, CISSP
National Security Corporation
gmhardy@nationalsecurity.com
+1 410.933.9333
@g_mark