ShmooCon 9 Badge Puzzle

Darth Null, February 2013

- Changed it up a little
  - More people to play
  - Not as much tough crypto
  - Parallel stages
  - More chances for people to win
- Multi-stage puzzle
  - Letters from each stage's solution form key
  - Key solves last stage

Stage 1

WELComE TO SHMoOCON IX!
AS a SPeCIAL trEAt, wE hAVE A mUlTI-STagE PUZZLe tHAT YOu cAN SOlVe. gOoD LuCk!

(thanks to G. Mark for this stage)

Bacon Cipher

- A form of steganography
- Five-letter groups, upper- vs lower-case
- WELComE TO S.... --> AAAAb bAAAA
- Read as binary...
- ...but I/J and U/V are shared symbols, so not quite a direct mapping

First Stage Answer

Stage 9 Key

Stage 2

2

	B		A		S			
		A					P	O
I				L			B	
	P				B	I		N
			P					
O		N	S				L	P
							S	
S	N	I		G		O		
			I					L

(the letters in the shaded squares will spell out the answer)

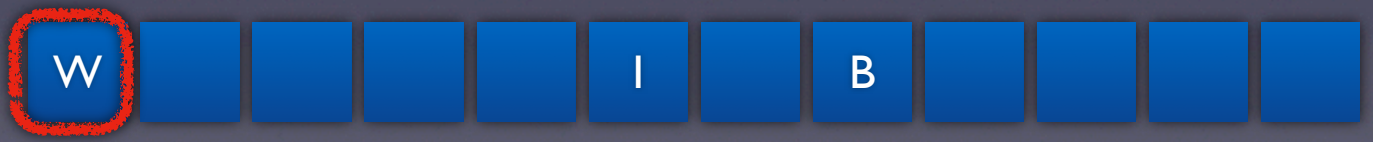
N	B	O	A	P	S	L	I	G
G	L	A	N	B	I	S	P	O
I	S	P	G	L	O	N	B	A
L	P	S	O	A	B	I	G	N
B	I	G	P	N	L	A	O	S
O	A	N	S	I	G	B	L	P
A	G	L	B	O	N	P	S	I
S	N	I	L	G	P	O	A	B
P	O	B	I	S	A	G	N	L

Stage 3

3 Dor dt lsr ydnarkl wdoljbflcdok ld er krro bl b KsmddWdo: b hbk fdqrjra yrbt eydqrj.

```
One of the loudest contraptions to
be seen at a ShmooCon: a gas powered
leaf blower.
```

- Silly bit - alphabet key:
  - BEWARTHSCUIYMODFGJKLNPQVXZ
  - “Beware the Security Moose”



Stage 4

4

Collected Deckard

EX-TERM-IN-ATE

Ripley's Ship

Became self-aware in 1997

Directed 2001

Brown's Capacitor

Father of the clones

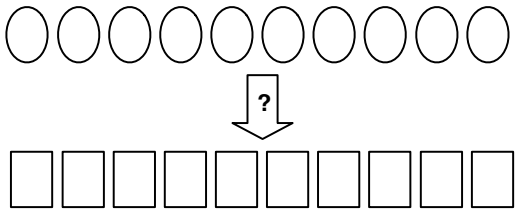
OF	YN	FL	KU
ET	GA	ETT	UX
LE	KS	FF	SK
TRO	MO	BR	ICK
JA	DA	NG	NOS

Directions

Using the tiles on the right, build the words indicated by the hints above. Use each tile only once.

Then copy the letters in circles to the circles below (in top-down, left-right order).

Last, decode the final answer.



4

Collected Deckard — G A F F

EX-TERM-IN-ATE — D A L E K S

Ripley's Ship — N O S T R O M O

Became self-aware in 1997 — S K Y N E T

Directed 2001 — K U B R I C K

Brown's Capacitor — F L U X

Father of the clones — J A N G O F E T T

OF	YN	FL	KU
ET	GA	ETT	UX
LE	KS	FF	SK
TRO	MO	BR	ICK
JA	DA	NG	NOS

Directions

Using the tiles on the right, build the words indicated by the hints above. Use each tile only once.

Then copy the letters in circles to the circles below (in top-down, left-right order).

Last, decode the final answer.

G L E T Y T R I U J

?

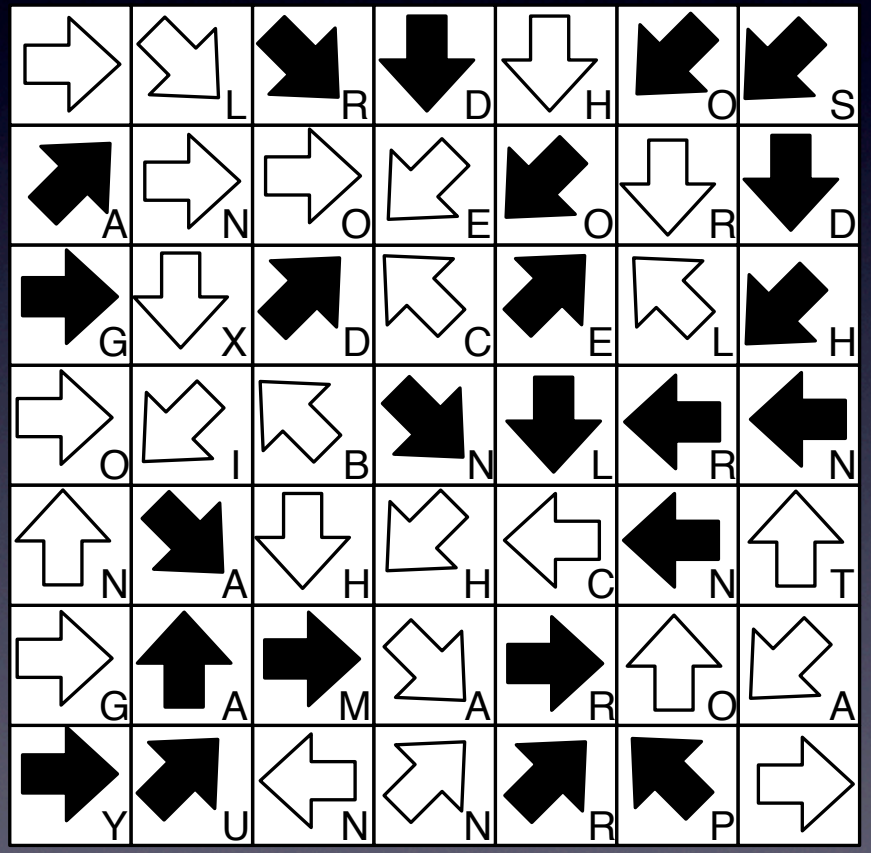
P U N C H C A R D S

W C I B

Stage 5

5

START



EXIT

Directions

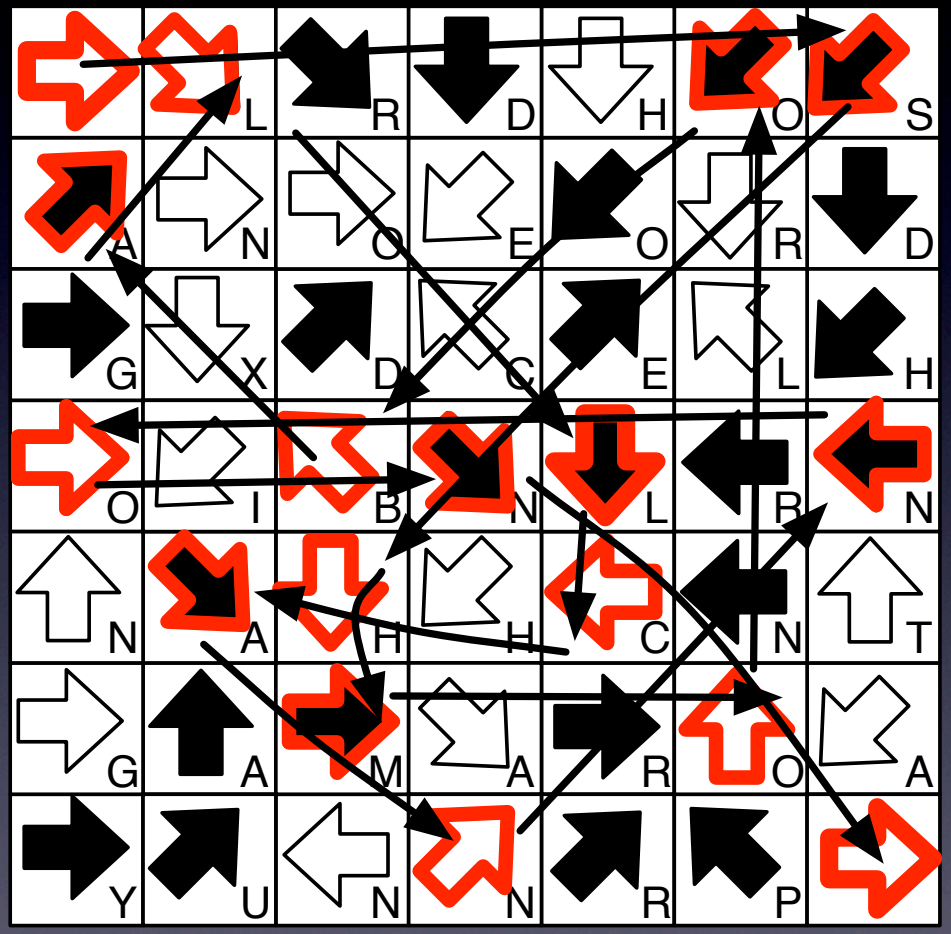
Hop from square to square in the direction of the arrow. Can jump as many squares as you like, but MUST land on an arrow of the opposite color.

The object is to get to the exit, spelling out the answer as you go.

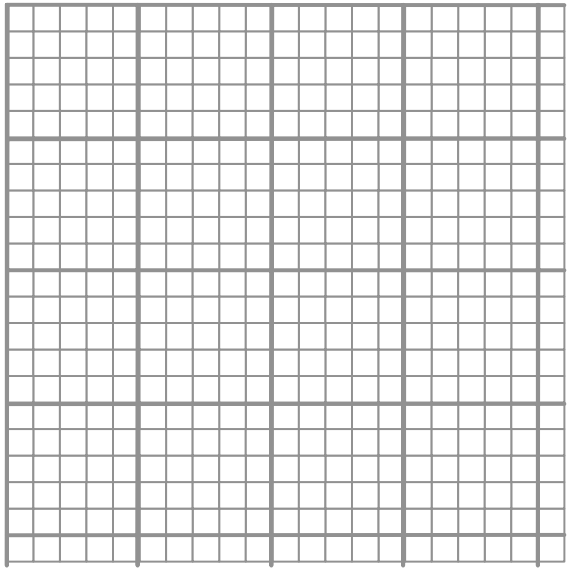
Near Misses

- SHMOOCOD - misspelled, color fail
- RED HERRINGX - doesn't exit
- DARTH NUL - infinite loop
- SHMOOGANOGRAPHU - *almost*

ShmooBall Cannon



Stage 6



7-1-2-7
1-1-3-1-1
1-3-1-2-2-1-3-1
1-3-1-1-1-1-3-1
1-3-1-1-1-1-3-1
1-1-1-1-1
7-1-1-1-7
2-2
3-8-2-1
5-1-1-2-3
2-1-2-5-2
2-1-1-1-1
1-2-1-1-1-2-1
1-3-2-1
7-1-1-4-2
1-1-5
1-3-1-2-1-2-1
1-3-1-4-2-1
1-3-1-1-3-4-1
1-1-1-1-1-1
7-1-1-1-2

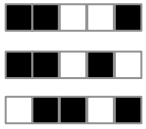
7-1-7
1-1-2-1-1
1-3-1-2-1-3-1
1-3-1-4-1-3-1
1-3-1-5-1-3-1
1-1-2-1-1
7-1-1-1-7
1-1
1-4-4-3
4-2-1-3
1-1-1-1-4-1-3
4-3-1-4-1
1-1-4-1-4-3
1-1
7-1-1-1-1
1-1-2-3-2-1
1-3-1-6-3
1-3-1-1-1-1
1-3-1-2-1
1-1-2-1-2-2
7-4-1-1-1

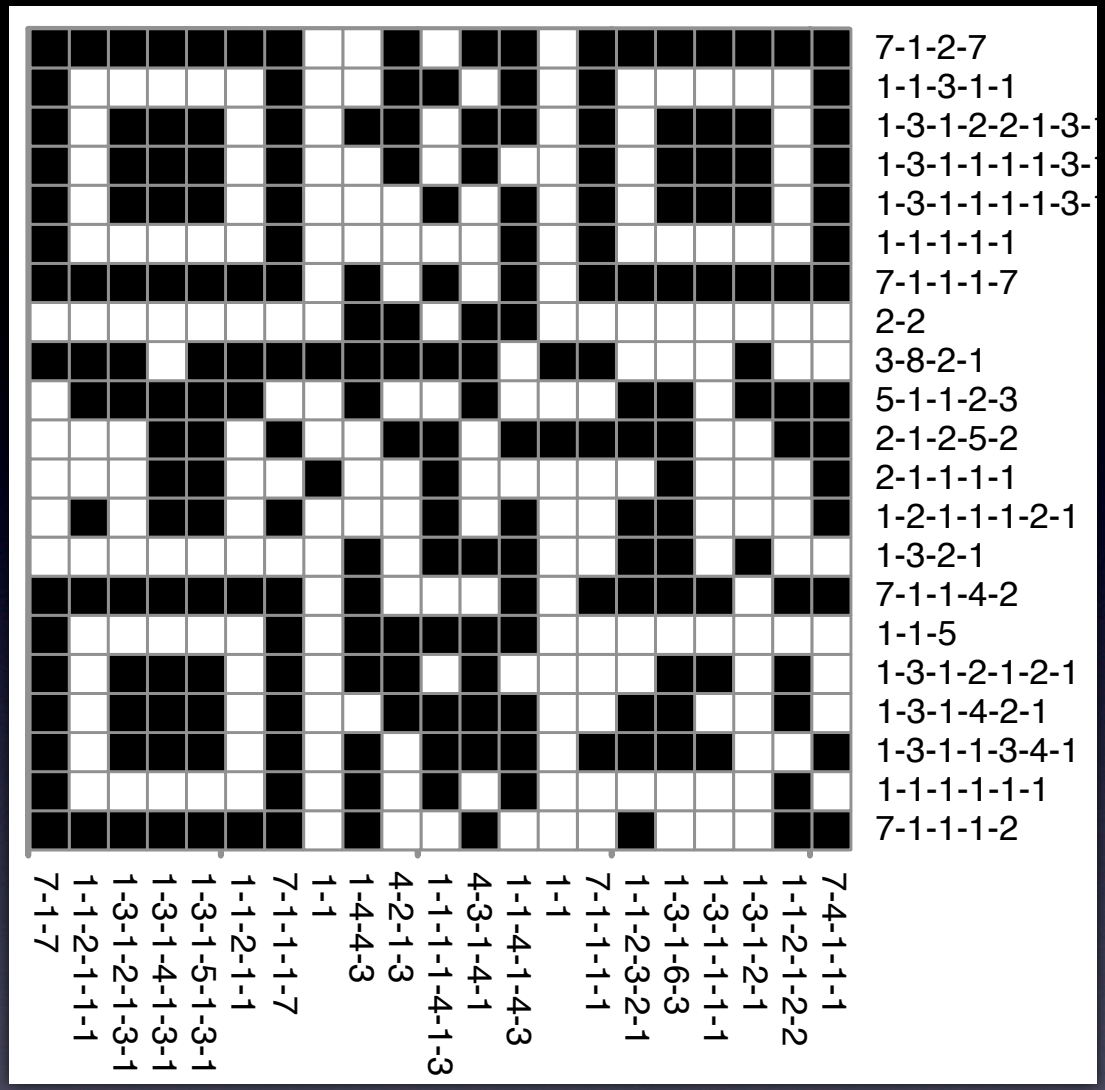
6

Directions

The numbers next to each row and column indicate the size of groups of contiguous black pixels. Fill in the pixels.

For example: "2-1" in a five-square row could indicate any of three possible arrangements:



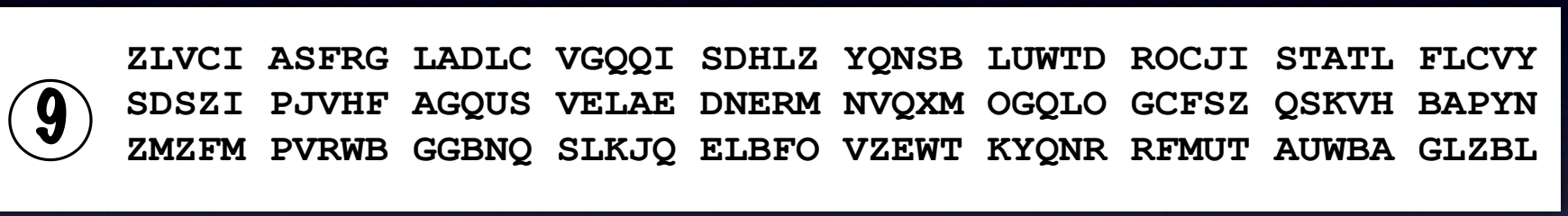


"Snowmageddon!"

W C I M B C

Update on Stage 9

W			C		I	M	B		C		



- Have half the key figured out
- Not a big stretch to guess it's a Vigenère cipher
- Know length, have half the letters: Should be easy now!

Decryption So Far

```
DLVAI SGERE LAHLC TGIEH SBHLD YQLST ZTWRD RSCJG SLOSL DLCZY
SBSRW OJTHF EGQSS NSKAC DNIRM LVILL OEQLS GCDSR ERKTH BEPYL
ZENEM NVRAB GEBFE RLIJQ ILBDO NNDWR KYUNR PFEIS ASWBE GLXBD
```

Stage 7


ShmooCon 2013
FEB 15 - 17
ALL DAY PASS
0dGhFRwWub2lzZQ
DISCLAIMER: Information security is inherently dangerous. You may get pwned, doxed, trolled, disenfranchised, and heartbroken. The wearer of this ticket assumes all risks associated with this career / hobby / psychosis. ShmooCon Logistics LLC, ShmooCon volunteers, ShmooCon speakers, hotel staff, relatives, interested parties, disinterested parties, clients, sponsors, followers, and those that have "linked" you on Linked-In will not be held responsible for any injuries, mental or physical, that you may incur. Please keep your hands inside the ride at all times. Do not taunt the ShmooBall. Don't litter. Be aware of your surroundings, help those in need, educate those who wish to learn, be kind to others, and participate constructively. Don't wear a fanny pack. And above all else, please enjoy yourself.
Hyatt Regency Washington DC
SPEAKER

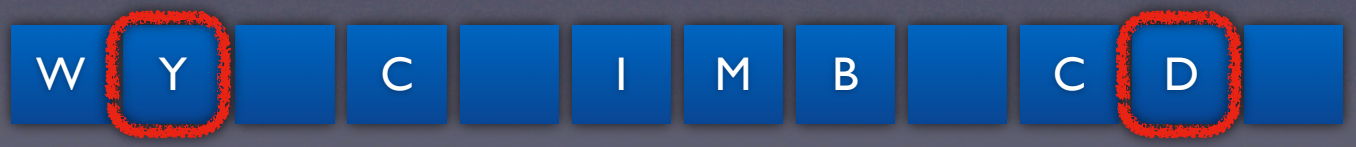
```
dHVyREVFbnV    WxBUkV3aXBF
wQVJFdGhlV0    SD9lb3VFU1N
hZc2lnRUVuY    0dGhFRWVubZlzZQ
```

- Six badges. Base-64.
- Put in wrong order, get gibberish

turDEEnupAREtheWHYsigEEnal

AREwipEH?eouESSttthEEenoise

DRY ERASE



Stage 8

Message Intercept

blemeieiebnomtapelvOehpOoeenlosiWtrbysas
ebehmvrSdrahiheuiwtawrMnhheuvmsmoeiteEta
[61 59 29]

Message Intercept

uOgtgEgeiealrsrlMnphahrttsbuseloIesunird
yisoSsnettseydbnvutrtaectdunganissOnerei
[23 59 11]

Message Intercept

slmnnhOaStMibetfueahlndtneendOniOOteOdrn
rhmitOlelEhEttaStebmOidennokoogrhseMlmae
[59 67]

Message Intercept

ToDamyNnwittveseffSoudctratogiogTeoagueg
soOetoiityneoaavtOkioaemhsuaugtrMareEtng
[41 3]

Message Intercept

rrxtmhEuriohetttuieeiOhsknetaweoIgidwrTt
oshktorlnfnarllhetcnMIyikWvsyeeolaeStfkO
[79 79]

Message Intercept

wmeahiuhvecSeshOanateftshngpyaEuLBrrhDti
LawtletorertMhptisrhicaguigeeOtiiopoypty
[29 37]

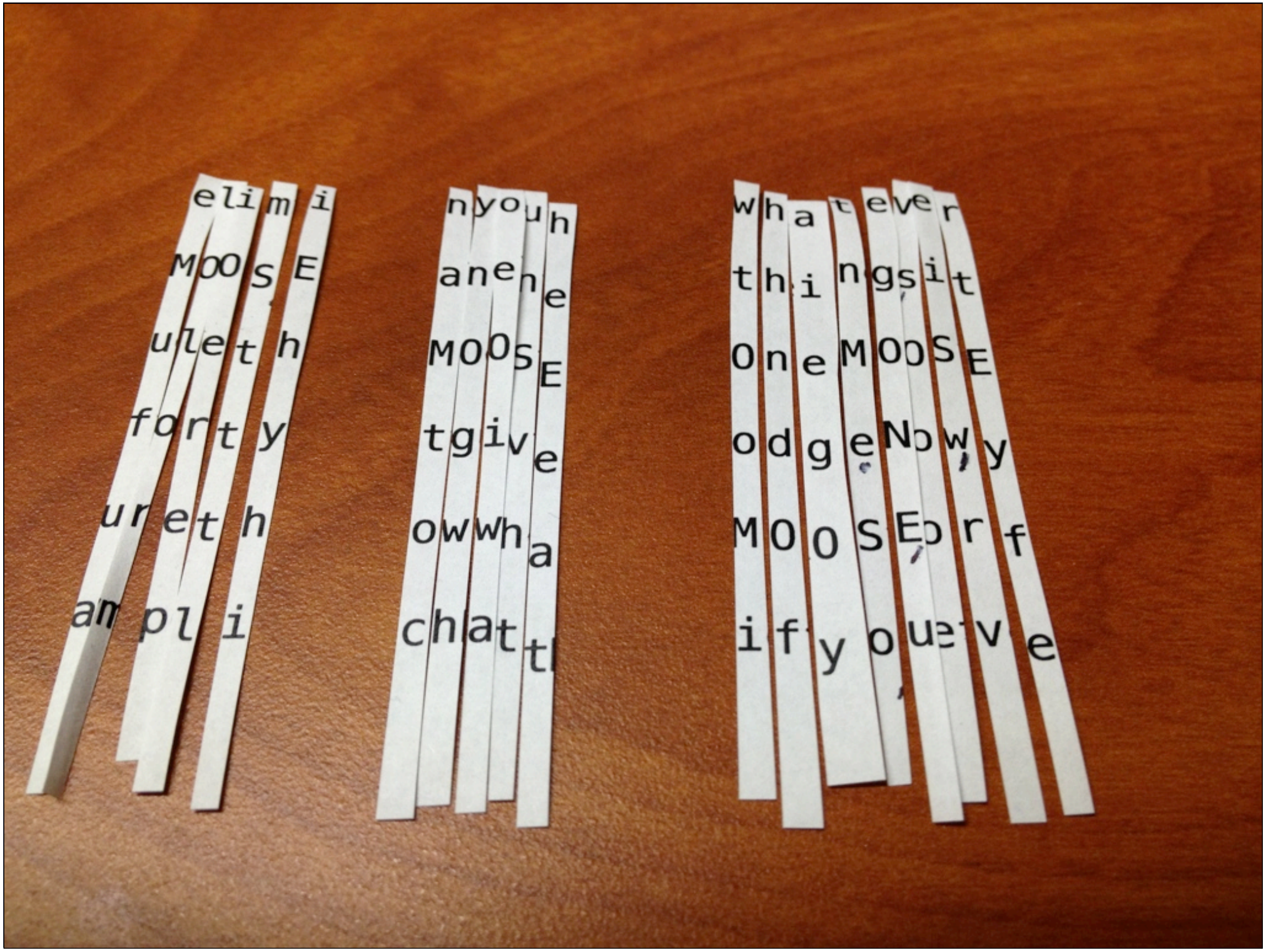
- Two step puzzle
- Step 1: Double Transposition Cipher
- Mistake 1: Same message length and same key
- Classic Cryptanalysis Method: “In Depth Attack”

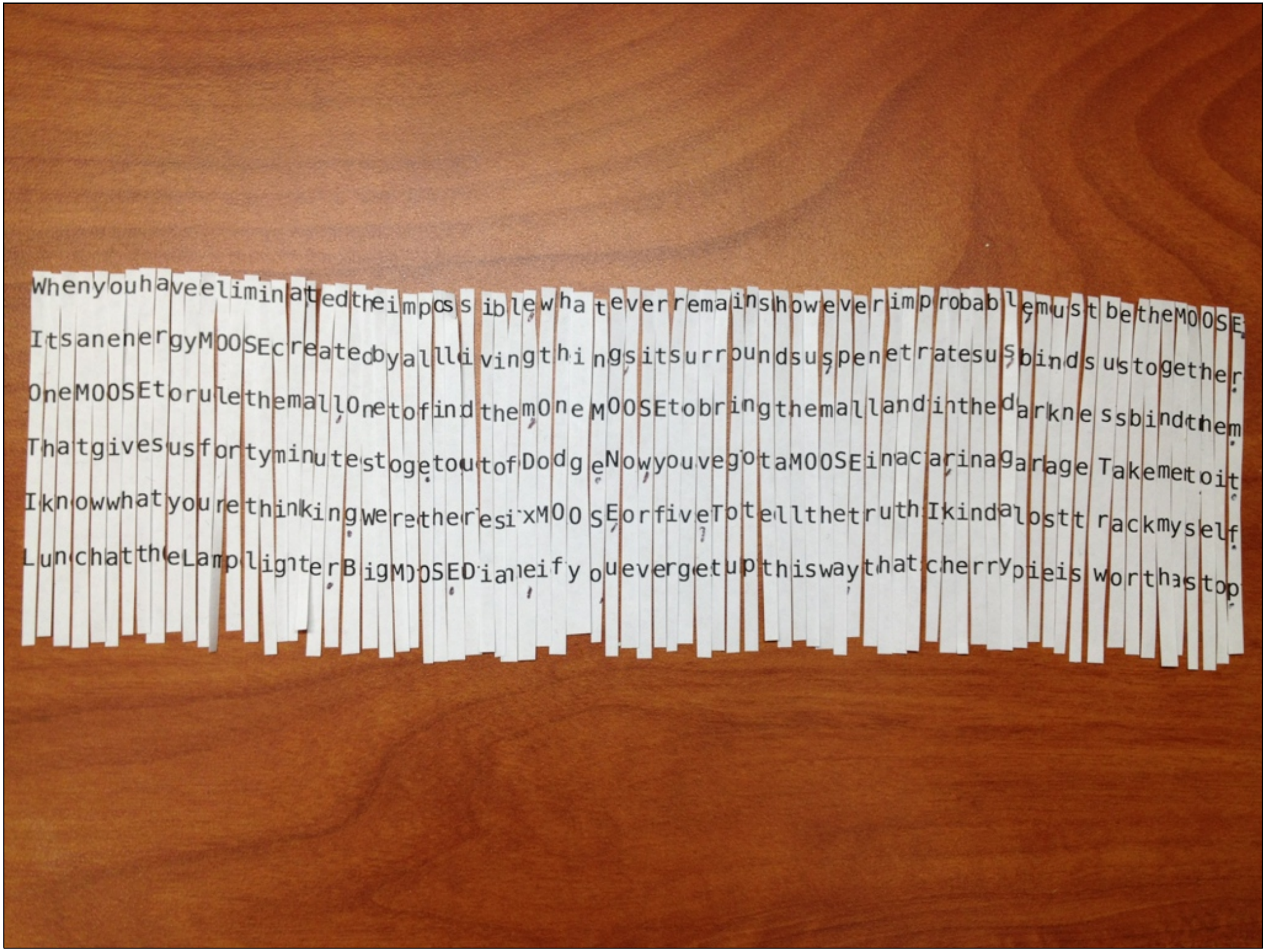
- Substitution: Change letters
  - A becomes Q, B becomes F, etc.
- Transposition: Shuffle letters around
  - SHMOO becomes OHMSO
- In-Depth: Same scramble pattern for each message

- Used frequently in World War II
- WWBD?
- Re-arrange letters to form word on one line...
- ....and you should see words form on the other 5.

```
blemeieiebnomtapelvOehpOoeenlosiWtrbysasebehmvrSdrahiheuiwtawrMnhheuvmsmoeiteEta
uOgtgEgeiealrsrlMnphahrttsbuseloIesunirdyisoSsnettseydbnvutrtaectdunganissOnerei
slmnnhOaStMibetfueahlndtneendOniOOteOdrnrhmitOlelEhEttaStebmOidennokoogrhseMlmae
ToDamyNnwittveseffSoudctratogiogTeoaguegsoOetoiityneoaavtOkioaemhsuaugtrMareEtng
rrxtmhEuriohetttuieeiOhsknetaweoIgidwrTtoshktorlnfnarllhetcnMIyikWvsyeeolaeStfkO
wmeahiuhvecSeshOanateftshngpyaEuLBrrhDtiLawtletorertMhptisrhicaguigeeOtiiopoypty
```


KLEENEARTH®


elimi
MOOSE
uleth
forty
ureth
ampli
nyouh
anene
MOOSE
tgive
owwha
chatt
whatever
thingsit
oneMOOSE
odgeNowy
MOOSErf
ifyouve


When you have eliminated the impossible whatever remains however improbable must be the MOOSE.
It's an energy MOOSE created by all living things its surrounds us penetrates us binds us together.
One MOOSE to rule them all, One to find them, One MOOSE to bring them all and in the darkness bind them.
That gives us forty minutes to get to out of Dodge Now you've got a MOOSE in a carina garage Take me to it.
I know what you're thinking Were there six MOOSE or five To tell the truth I kinda lost track myself.
Lunch at the Lamplighter Big MOOSE Diane if you ever get up this way that cherry pie is worth a stop.

Its an energy MOOSE created by all living things it surrounds us penetrates us binds us together.

One MOOSE to rule them all One to find them One MOOSE to bring them all and in the darkness bind them.

That gives us forty minutes to get out of Dodge. Now you've got a MOOSE in a car in a garage. Take me to it.

I know what youre thinking. Were there six MOOSE or five? To tell the truth I kinda lost track myself.

Lunch at the Lamplighter. Big MOOSE. Diane if you ever get up this way that cherry pie is worth a stop.

If you're curious, the keys used were

ACCEPT YOUR // MOOSEY FATE

- Second part
  - Numbers in brackets for each intercept
  - Letters from each plaintext

```
Its an energy MOOSE created by all living things it surrounds us
penetrates us binds us together.

[61 51 29]
```

  - 61 51 29 becomes OPS
  - “DRYWALL DROPSEY”

Stage 9

- Remember, we had:


```
DLVAI SGERE LAHLC TGIEH SBHLD YQLST ZTWRD RSCJG SLOSL DLCZY
SBSRW OJTHF EGQSS NSKAC DNIRM LVILL OEQLS GCDSR ERKTH BEPYL
ZENEM NVRAB GEBFE RLIJQ ILBDO NNDWR KYUNR PFEIS ASWBE GLXBD
```

- Now we have:

- "MOOSEY CRISTO" after a Ceaser shift

- Real concern people would decrypt too easily
- Wanted players to solve all the other stages first
- Also wanted special incentive for folks to attack it directly (potentially winning 2nd place)
- How to make it hard, just not impossible?

- Make the key random gibberish
- Spread letters from “easy” stages around
- Add garbage at the front of the plaintext

- Write the plaintext in German

- (but the secret words are English, so translation not strictly necessary)

DNXAU SGEZE ICHNE TSIEH ABEND ASLET ZTERA TSELG ELOST DIEZA
UBERW ORTEH EISSE N**SKIC APITO LHILL** WENNS IEDER ERSTE DERAL
LENEU NSTAD IENFE RTIGS INDDA NNDER HAUPT PREIS ISTDE INXND

DNX AUSGEZEICHNET SIE HABEN DAS LETZTE RATSEL GELOST DIE ZAUBERWORTE HEISSEN **SKI CAPITOL HILL** WENN SIE DER ERSTE DER ALLE NEUN STADIEN FERTIG SIND DANN DER HAUPTPREIS IST DEIN XND

Ausgezeichnet! Sie haben das letzte ratsel gelost. Die zauberworte heissen "Ski Capitol Hill." Wenn Sie der Erste der alle neun stadien fertig, sind dann der Hauptpreis ist dein.

Excellent! You have solved the last riddle. The magic words are "Ski Capitol Hill." If you are the first to finish all nine stages then the grand prize is yours!

Congratulations!

- Stage 1: Nat Puffer
- Stage 2: Matthew Bockneck
- Stage 3: Matthew Bockneck
- Stage 4: Matthew Bockneck
- Stage 5: Matthew Bockneck
- Stage 6: Mystik

Congratulations!

- Stage 7: Mike Herms
- Stage 8: Tyler Vernon

Congratulations!

- Grand Prize Winner:
  - Matthew Bockneck
- First to solve all nine stages

- Free ticket to ShmooCon X

Thanks for playing!