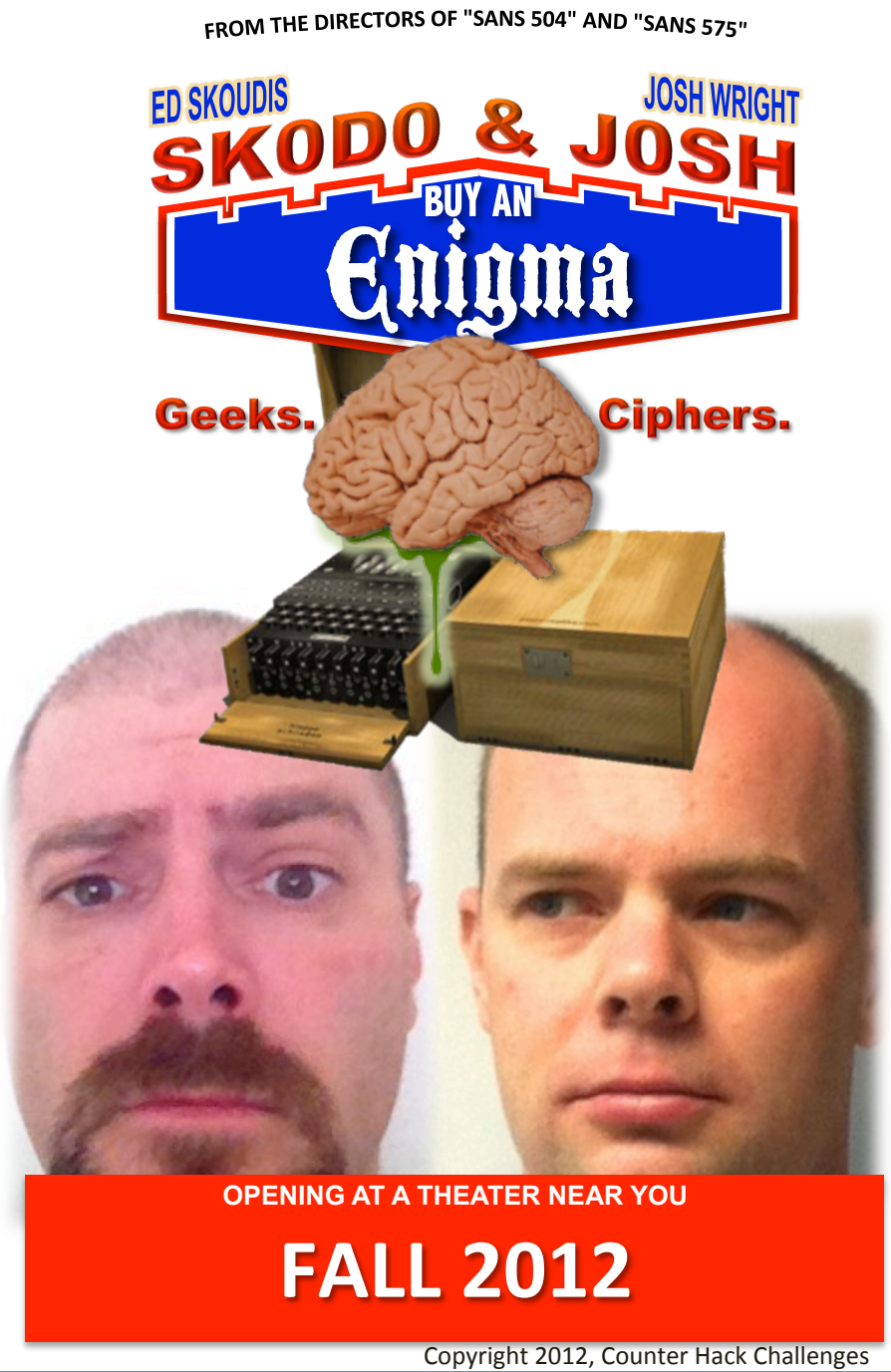
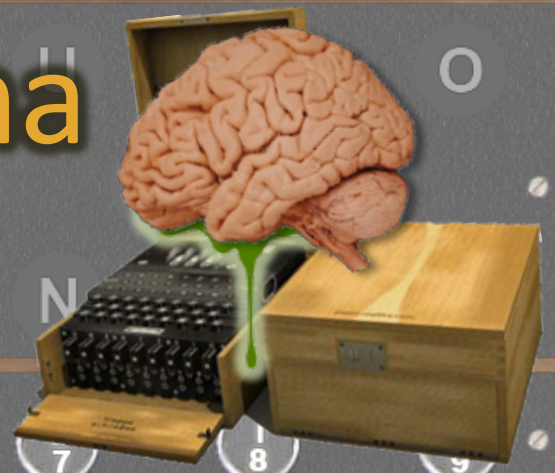


Please Keep Your Brain Juice Off My Enigma

- A True Story -



By Ed Skoudis & Josh Wright

September 2012

Our Adventure

- What you are about to hear is a true story
- We'll start by providing a little history about one of the starring characters of the story, the Enigma Machine
- We'll then share a tale of our adventure in buying one

ENIGMA I

About the Enigma

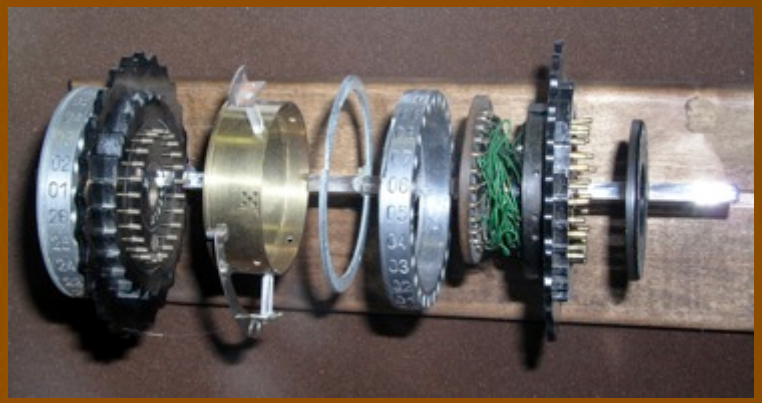
- Initially a business machine, later enhanced by the German Government for military use
- Mechanically implements a step-based substitution cipher
- Operator sets the reflector, plugboard, and the position and order of rotors as the key
- Variants of the Enigma used throughout the war

During the War

- The Enigma was relied upon for secret message delivery over Morse Code
- For the Allied Forces, the inability to decode messages led to significant loss of life and resources
- Cracked by Polish, British, Americans
  - Each supporting the former as more complex versions of the Enigma were adopted
  - Marian Rejewski (PL), Alan Turing (UK), Joseph Desch (US)
- According to Winston Churchill, cracking the Enigma shortened the war by two or three years
- An earlier end to the war saved million of lives on both sides

Enigma Cryptography

- Polyalphabetic substitution cipher using rotor scramblers
  - Eliminated use of character frequency analysis
  - Forced analyst shift from linguists to mathematicians
- Attempt at achieving Kerchoff's Principle
  - Prior to recovery of an Enigma, a formidable obstacle
- Keyspace calculations vary, theoretically 3 x 10^{114}

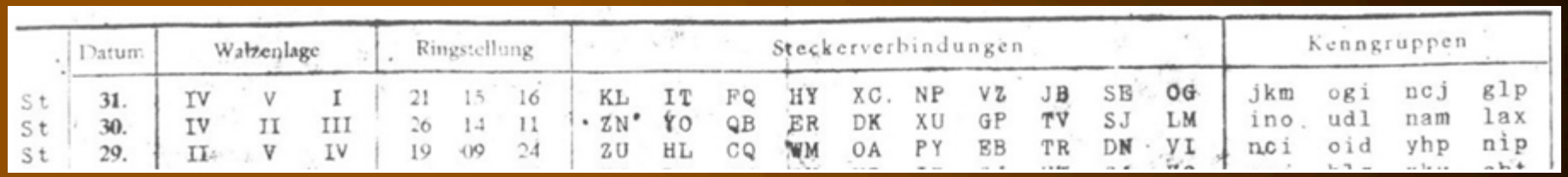


ENIGMA I

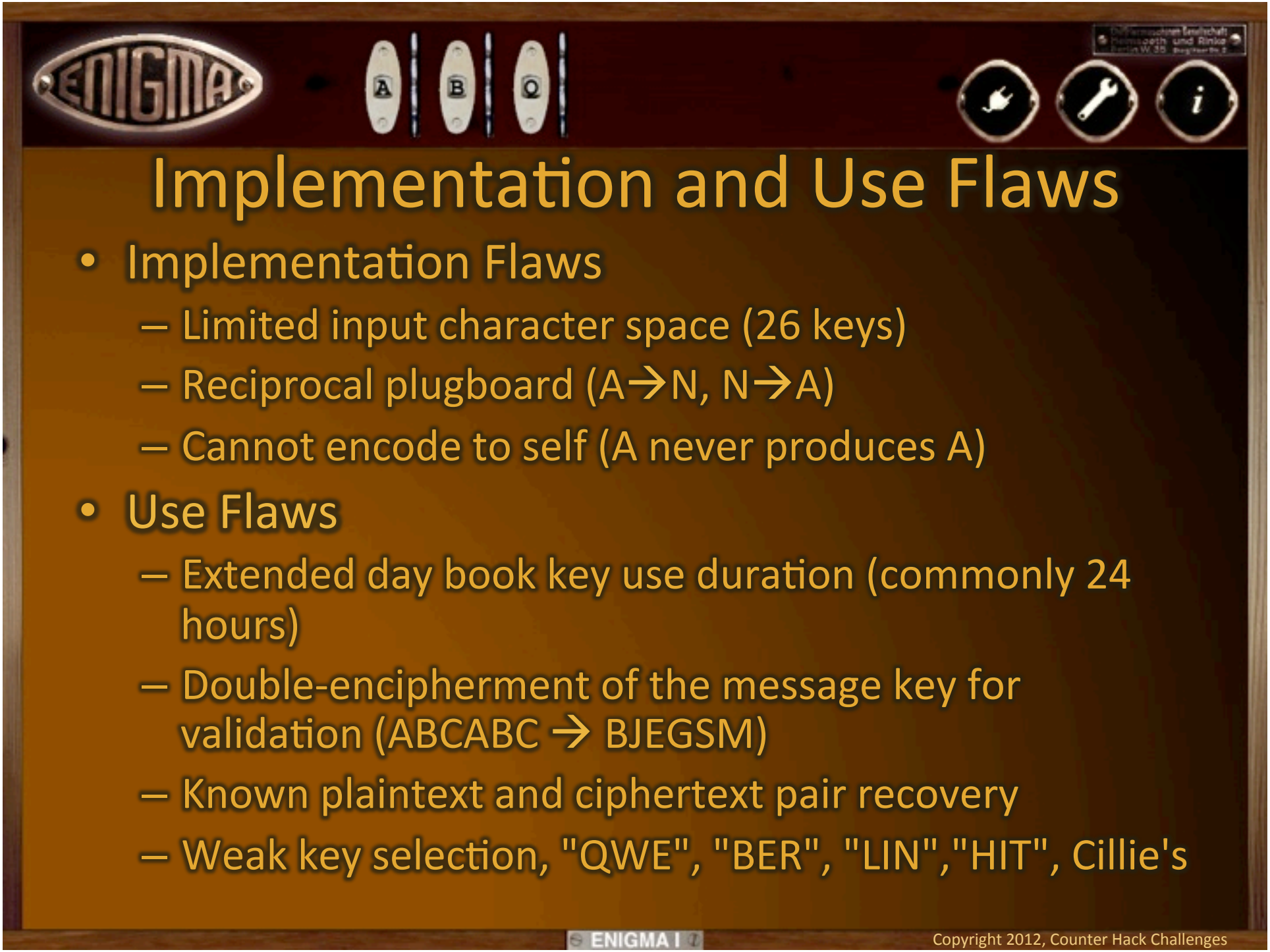
Enigma Keying Operation

- Operator would use the Day Book to set the initial Enigma settings
  - Walzenlage: choice and order of rotors
  - Ringstellung: ring setting of each rotor
  - Steckerverbindungen: plugboard letter pairs
- Operator would "randomly" choose three letters for the message key (spruchschlüssel)
  - Message key was sent twice as a MIC, then the ringstellung was changed to the message key
- Receiver would decode message key, validate MIC, then change the ringstellung to match and decrypt message
- This keying method mitigated statistical attacks from large data set TX, but introduced other weaknesses from weak message key selection

Incoming Message: ORCNCCTWPTZTRS	Decrypt Message Key: ORCNCC → JLWJLW	Change rotors to JLW	Decrypt Message: TWPTZTRS → HELLOXED



	Datum	Walzenlage			Ringstellung			Steckerverbindungen										Kenngruppen			
St	31.	IV	V	I	21	15	16	KL	IT	FQ	HY	XC	NP	VZ	JB	SB	OG	jkm	ogi	ncj	glp
St	30.	IV	II	III	26	14	11	ZN	YO	QB	ER	DK	XU	GP	TV	SJ	LM	ino	udl	nam	lax
St	29.	II	V	IV	19	09	24	ZU	HL	CQ	WM	OA	PY	EB	TR	DN	VI	nci	oid	yhp	nip

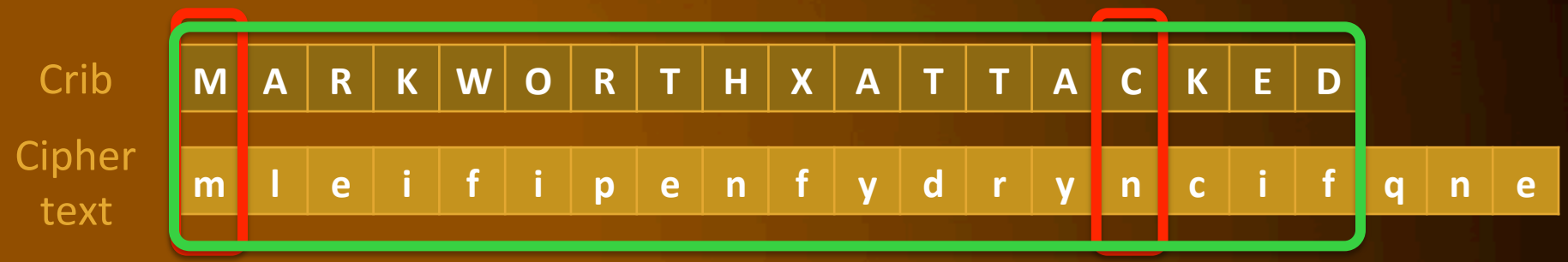


Implementation and Use Flaws

- Implementation Flaws
  - Limited input character space (26 keys)
  - Reciprocal plugboard (A→N, N→A)
  - Cannot encode to self (A never produces A)
- Use Flaws
  - Extended day book key use duration (commonly 24 hours)
  - Double-encipherment of the message key for validation (ABCABC → BJEGSM)
  - Known plaintext and ciphertext pair recovery
  - Weak key selection, "QWE", "BER", "LIN","HIT", Cillie's

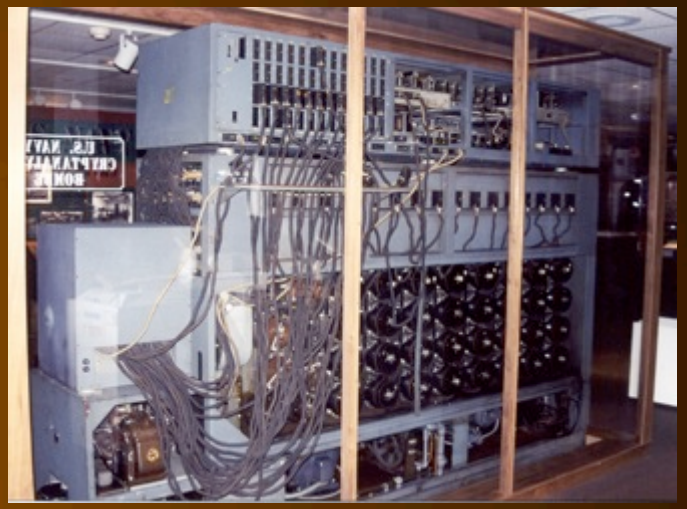
Use of Cribs

- A crib is plaintext content believed to be present in observed ciphertext
- Allows an analyst to search for valid key
- Weather station reports, test transmissions, raised submarine retransmissions
  - "KEINEXBESONDERENXEREIGNISSE"
- Later, Allied forces used Gardening to plant cribs



Bombe Machine

- Developed and enhanced by Polish, then British, then Americans (NCR/Dayton); staffed by Navy Waves
- Brute-forced rotor selection, position and plugboard configuration using cribs
  - Searching for workable circuits with no conflicting self-encoded characters in closed circuits (voltage test)



Historical Significance

- Amazing story about collaborative (if not always friendly) cryptographic analysis
  - Success of Enigma break remained a secret until 1974!

- Heroic mathematicians, soldiers, and sailors who gave their lives to the cause
- Inspiring role of women (British Wrens and Navy Waves)
- Cryptographic attacks we still use today!

Wouldn't It Be Cool…

- To have your own Enigma machine?
- Every five years or so, one comes up for sale on eBay
- You can buy parts (rotors and plug board cables)
- But, what about a whole Enigma?
- In March 2011, I toured the National Cryptologic Museum near Fort Meade
  - I asked the curator about having someone build a reproduction… He hooked me up with Jim Oram
  - Mr. Oram has been working on a faithful reproduction for over a decade, and has spent huge amounts… still not complete

Enter Yori

- Yori Kvitchko was teaching the SANS 504 class in June 2011, when a student mentioned he knew of a guy selling an Enigma… Dr. David
- I contacted Dr. David, who was acting as a broker between buyers and an unnamed seller
- We negotiated back and forth, getting close to finalizing a plan for mid-July 2011
- During the discussions, I learned that the seller was Dr. Tom
  - Retired college professor
  - Author of a book on Enigmas… they gave me a free copy

But Then…

- My wife got sick
- On June 29, 2011, doctors at Sloan told us her cancer returned
- She needed major surgery, chemo, radiation, and a lot of time to recover
- Not knowing the amount of my time would be needed to take care of her and the kids (to say nothing of the medical expenses), I called off the deal
- Dr. David and Dr. Tom were very gracious
  - They let me keep the free book ☺

A Year Passes

- It was a tough year
  - Thank you to all my friends for their well wishes, prayers, and support
- But, by July 2012, my wife was doing much, much, much better
  - I am so thankful
- I finally contacted Dr. David on July 19, 2012
  - "Long Time No Speak"
  - Got any Enigmas for sale?

Choices

- Four Enigmas to choose from!
- Many discussions and debates with my friends
  - Machine serial numbers (lower implies an earlier system)
  - Rotor serial numbers (mismatched numbers from the machine itself, plus for rotors I-III and IV/V)
  - Wear and tear, rust, splotches, etc.
  - The color of the wooden box
- Oh, and his best Enigma was in the final stages of negotiation with the Brazilians
  - I blame Mike Poor
- And, then, there was the idea of whether this was too crazy

The Seller

- Throughout our negotiations, I got to know Dr. Tom much better
- A fascinating gentlemen
- Very interested in education, technology, history
- A quirky sense of fun and adventure
- He sent me his Christmas cards

Some Christmas Cards

My Own Christmas Cards

```
# nmap -PN -sX 10.10.10.45 -p 79-81

Starting Nmap 5.21 ( http://nmap.org ) at 2010-12-25 15:27 EDT
Nmap scan report for 10.10.10.45
Host is up (0.0018s latency).
PORT    STATE         SERVICE
79/tcp closed         finger
80/tcp open|filtered http
81/tcp closed         hosts2-ns
MAC Address: 00:50:56:17:CF:45 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 14.28 seconds
```

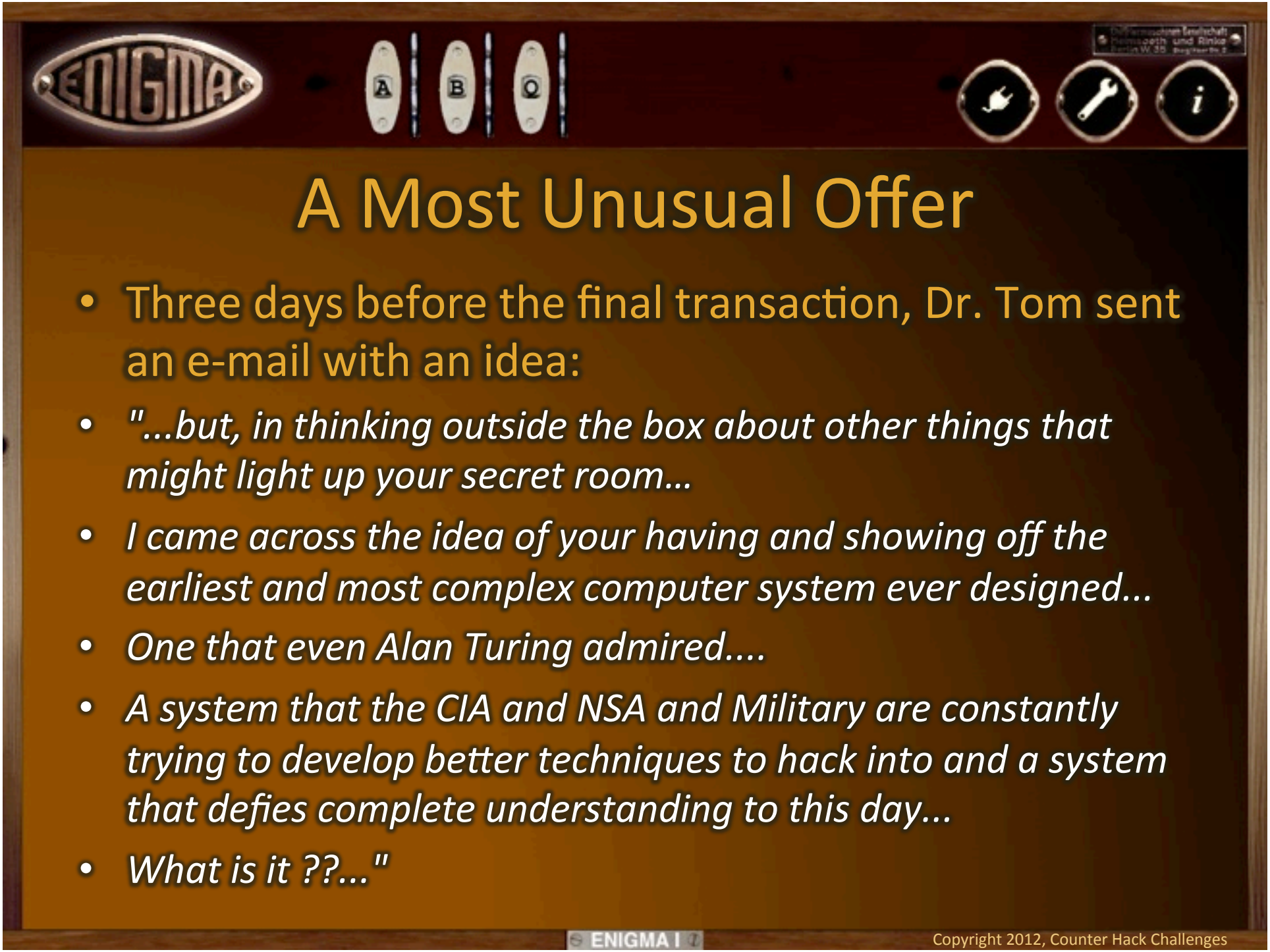
```
# hping --fin --push --urg --count 3 10.10.10.45 -p ++79
HPING 10.10.10.45 (eth0 10.10.10.45): FPU set, 40 headers + 0 data bytes
len=46 ip=10.10.10.45 ttl=64 DF id=0 sport=79 flags=RA seq=0 win=0
rtt=0.8 ms
len=46 ip=10.10.10.45 ttl=64 DF id=0 sport=81 flags=RA seq=2 win=0
rtt=2.9 ms

--- 10.10.10.45 hping statistic ---
3 packets tramitted, 2 packets received, 34% packet loss
round-trip min/avg/max = 0.8/1.8/2.9 ms
```

```
# scapy
Welcome to Scapy (2.1.1)
>>> sr1(IP(dst="10.10.10.45")/TCP(dport=(79,81),flags="FPU"),timeout=1)
Begin emission:
.*Finished to send 3 packets.
*..
Received 5 packets, got 2 answers, remaining 1 packets
<IP  version=4L ihl=5L tos=0x0 len=40 id=0 flags=DF frag=0L ttl=64
proto=tcp chksum=0xd18e src=10.10.10.45 dst=10.10.75.1 options=[] |<TCP
sport=finger dport=ftp_data seq=0 ack=1 dataofs=5L reserved=0L flags=RA
window=0 chksum=0x462b urgptr=0 |<Padding
load='\x00\x00\x00\x00\x00\x00' |>>>
```

A Deal

- We finalized the deal
- The plan was for Josh Wright and me to drive to his farm and inspect two of the Enigmas, choosing which one we liked best for purchase
  - A seven-hour drive each way for Ed
  - A four-hour drive each way for Josh
- Dr. Tom and his wife would serve "a delightful" lunch, show us the machines, and let us decide
  - He'd also throw in some nice extras: telegraphy keys, books, etc.
- The date was set: August 16, 2012

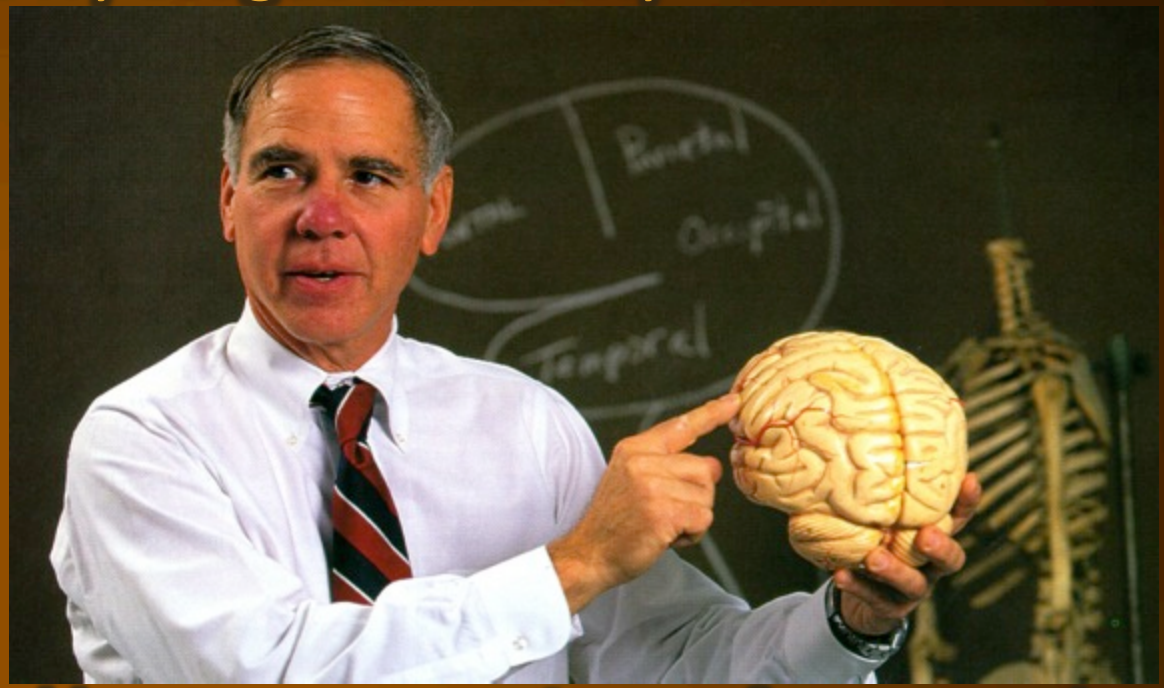


A Most Unusual Offer

- Three days before the final transaction, Dr. Tom sent an e-mail with an idea:
- *"...but, in thinking outside the box about other things that might light up your secret room…*
- *I came across the idea of your having and showing off the earliest and most complex computer system ever designed...*
- *One that even Alan Turing admired....*
- *A system that the CIA and NSA and Military are constantly trying to develop better techniques to hack into and a system that defies complete understanding to this day...*
- *What is it ??..."*

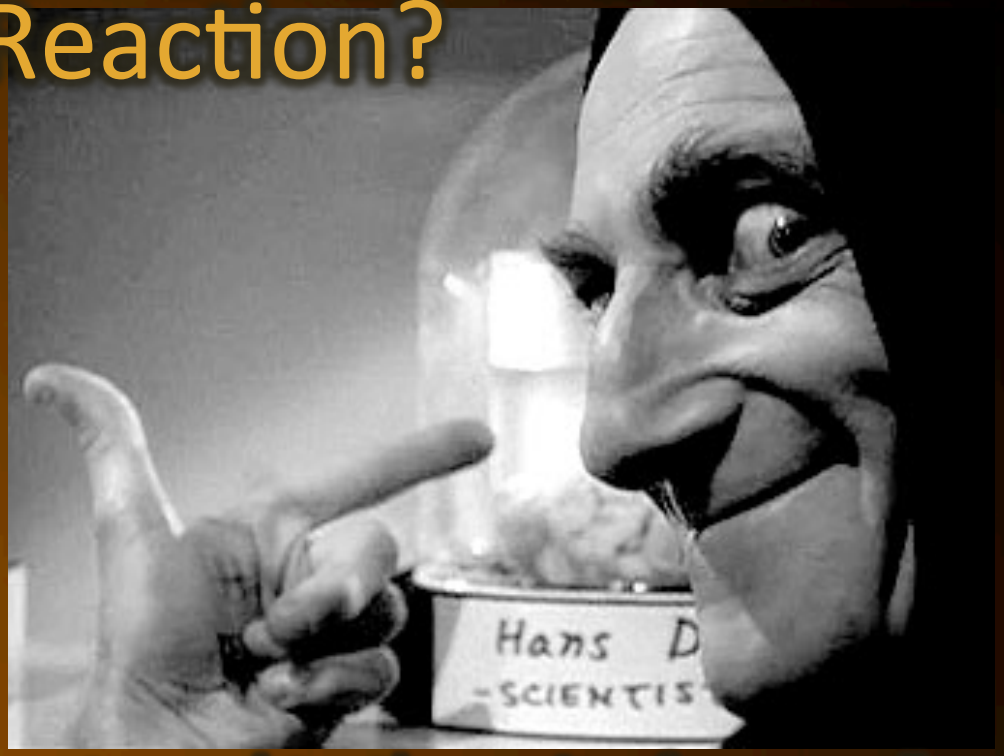
A Brain for the Secret Room

- Dr. Tom taught neuroscience and brain anatomy at a major Ivy League university



- He had kept some specimens for research and education… and offered me one for the Secret Room!

My Reaction?



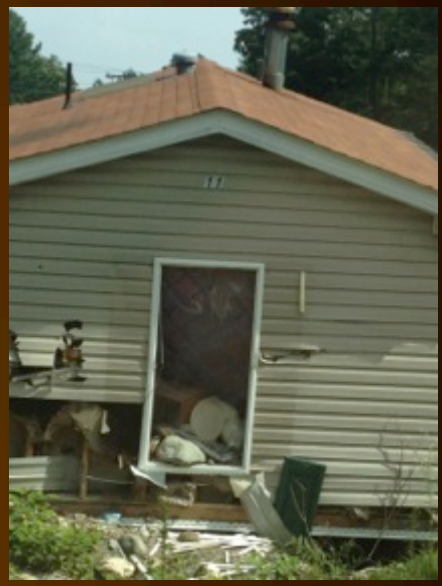
- "Ummm… thank you so much…"
- "But, it would kinda creep me out to have a brain in the Secret Room next to me."
- "It took me 3 weeks to get used to the suit of armor."
- "Thanks, but we'll pass on this one."
- "Although, I do like the idea. We'll get a fake one for the Secret Room and put an 'Abbie Normal' sign on it."

What To Wear?

- We briefly debated what to wear
  - Ed in an Enigma T-Shirt?
  - Josh in an Turing T-Shirt?
- We opted to go with more conventional clothing
- But, we brought the Enigma and Turing shirts in our cars in case we changed our minds

Aug 16, 2012: Enigma Day

- Ed leaves house at 5 AM
- Josh leaves at 8 AM
- We saw many strange things on the journey



Up a Scary Road

We Arrive

- A nice farm house on the top of a mountain
- Tom and his wife are waiting
- He takes us on a tour of his collection, with his wife taking photos

Testing an Enigma Machine

- Before we would take delivery, we insist that we test the machine
- I explain to Tom, "I brought my other Enigma with me and I want to encode a message and make sure it decodes properly"
- I use the iPad Enigma app to encode "JOSHXWRIGHT"
- It decodes perfectly
- "Before, it might have been a box that looked like an Enigma… now, we know it's a *real* Enigma!"

A Truly Delightful Lunch

- We enjoy a nice lunch: sandwiches and fresh gazpacho soup made from their garden
- On nice china plates

Decision Time

- We go for a walk to decide between A2200 and A726… We finally decide: A726
- "So, should we ask him to see the brain?"

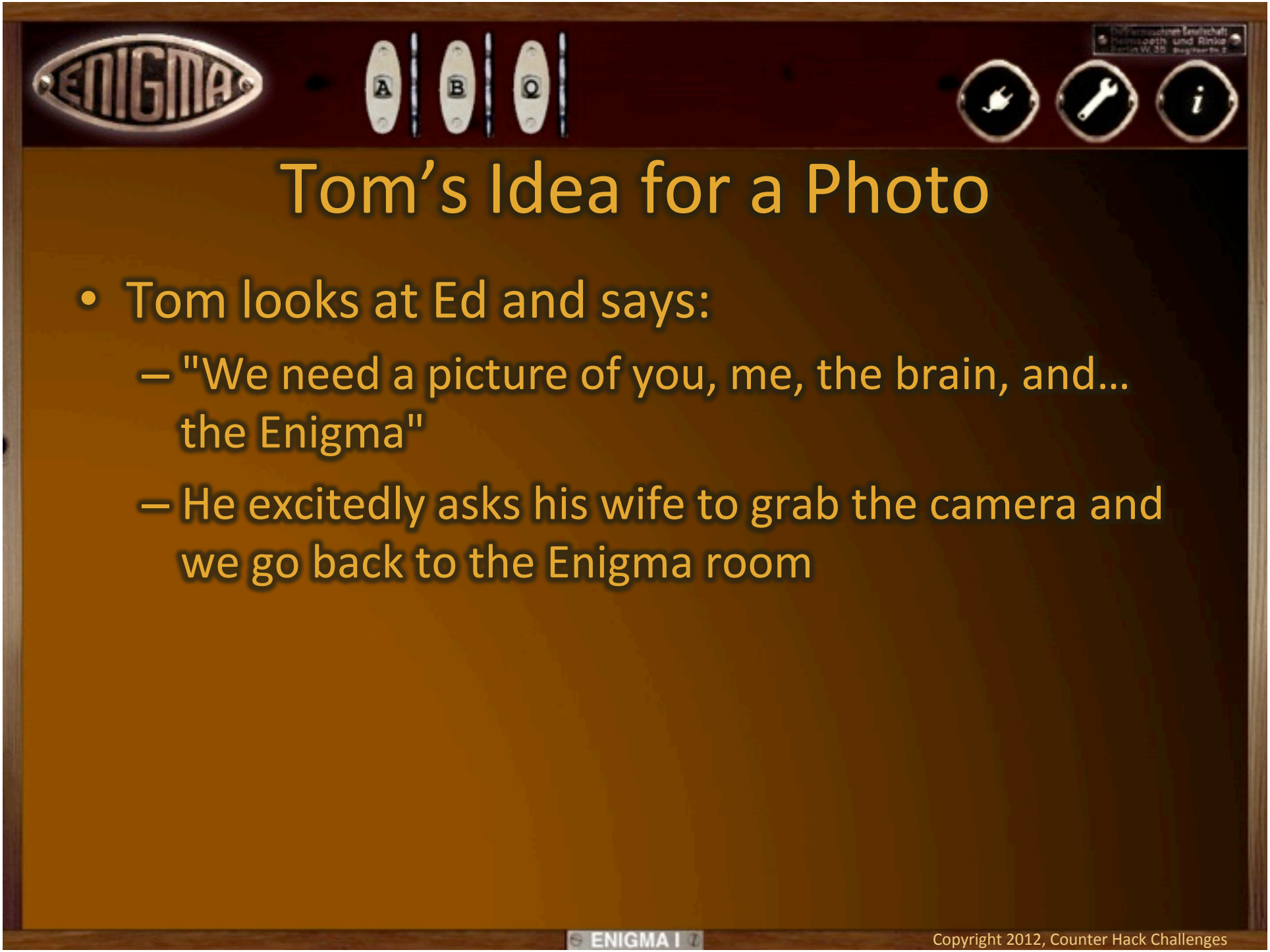
We Seal the Deal

"Uh… Can We See the Brain, Please?"

- We ask if we can see the brain, if it's not too much trouble
- Tom says, "I thought it would creep you out."
- "Yes, it probably will, but we figured we had to ask. Not to have it… just to see it"
- He puts on big yellow rubber gloves and excitedly runs into the other room to grab the brain

The Brain

- Tom asks his wife to grab a plate so he can better show us the brain
- Ed: "Gee, that's a nice china plate."
- Josh: "It's the same plate we just ate lunch on."



Tom's Idea for a Photo

- Tom looks at Ed and says:
  - "We need a picture of you, me, the brain, and… the Enigma"
  - He excitedly asks his wife to grab the camera and we go back to the Enigma room

"I Can’t Believe This Is Happening"

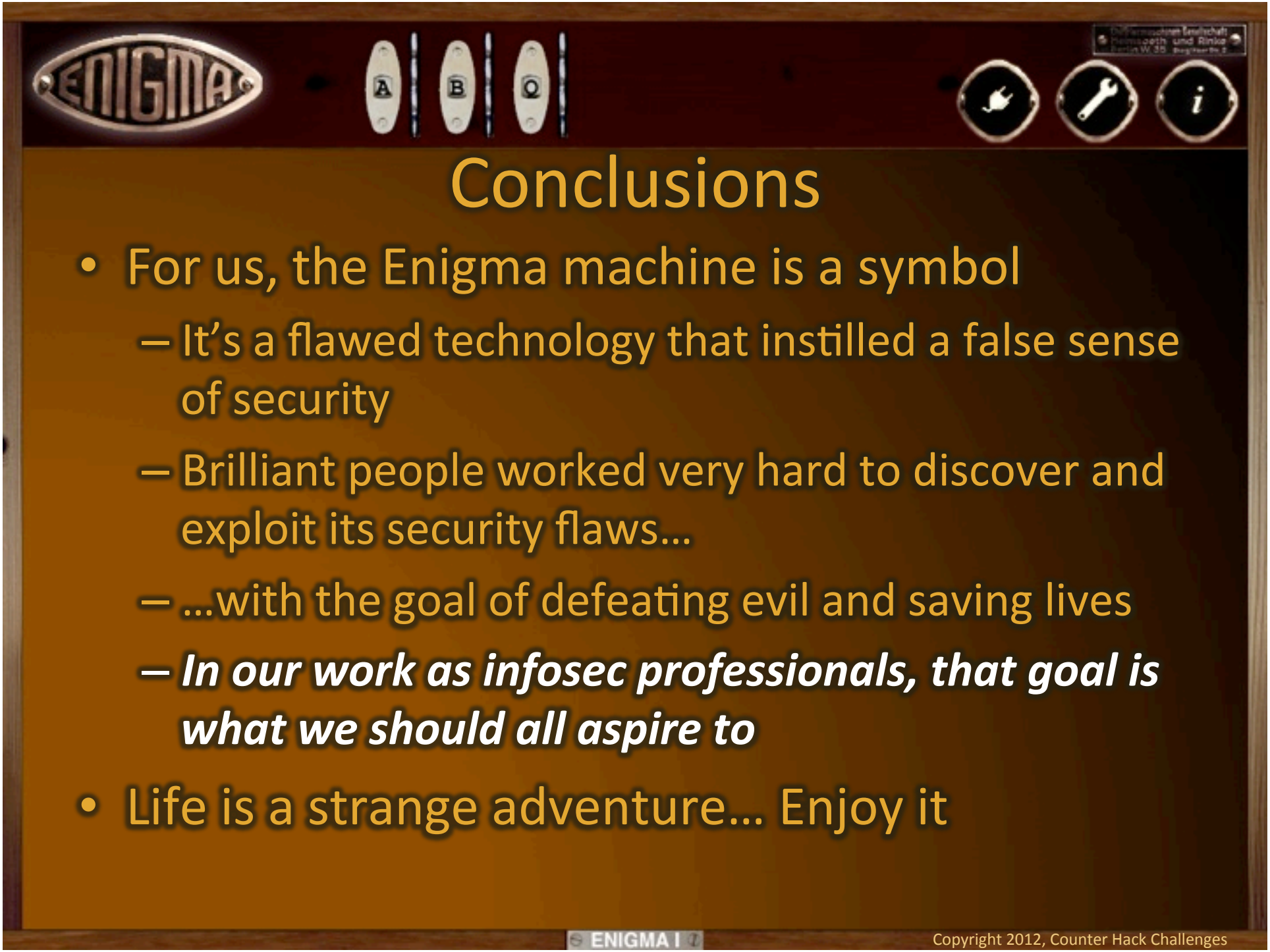
"Wait… What's That I See?"

Brain Juice!

- To get a better picture of the brain, Tom starts propping up the plate
- Liquid from the brain starts dripping on… the Enigma
- Ed kinda freaks out, and starts wiping up the brain juice, as Josh films
- Tom says, "It's no big deal"
- His wife says, "That Enigma survived World War 2… a little liquid isn't gonna hurt it."

But Then…

- The brain juice starts leaking onto the table
- Tom's wife: "That's my best table! This is serious!"
- She hurriedly wipes up the table
- The most surreal thing we've ever experienced



Conclusions

- For us, the Enigma machine is a symbol
  - It's a flawed technology that instilled a false sense of security
  - Brilliant people worked very hard to discover and exploit its security flaws…
  - …with the goal of defeating evil and saving lives
  - ***In our work as infosec professionals, that goal is what we should all aspire to***
- Life is a strange adventure… Enjoy it