Cryptography in WWI

Datto Engineering

Presented By: Fred Mora – October 2014

Agenda

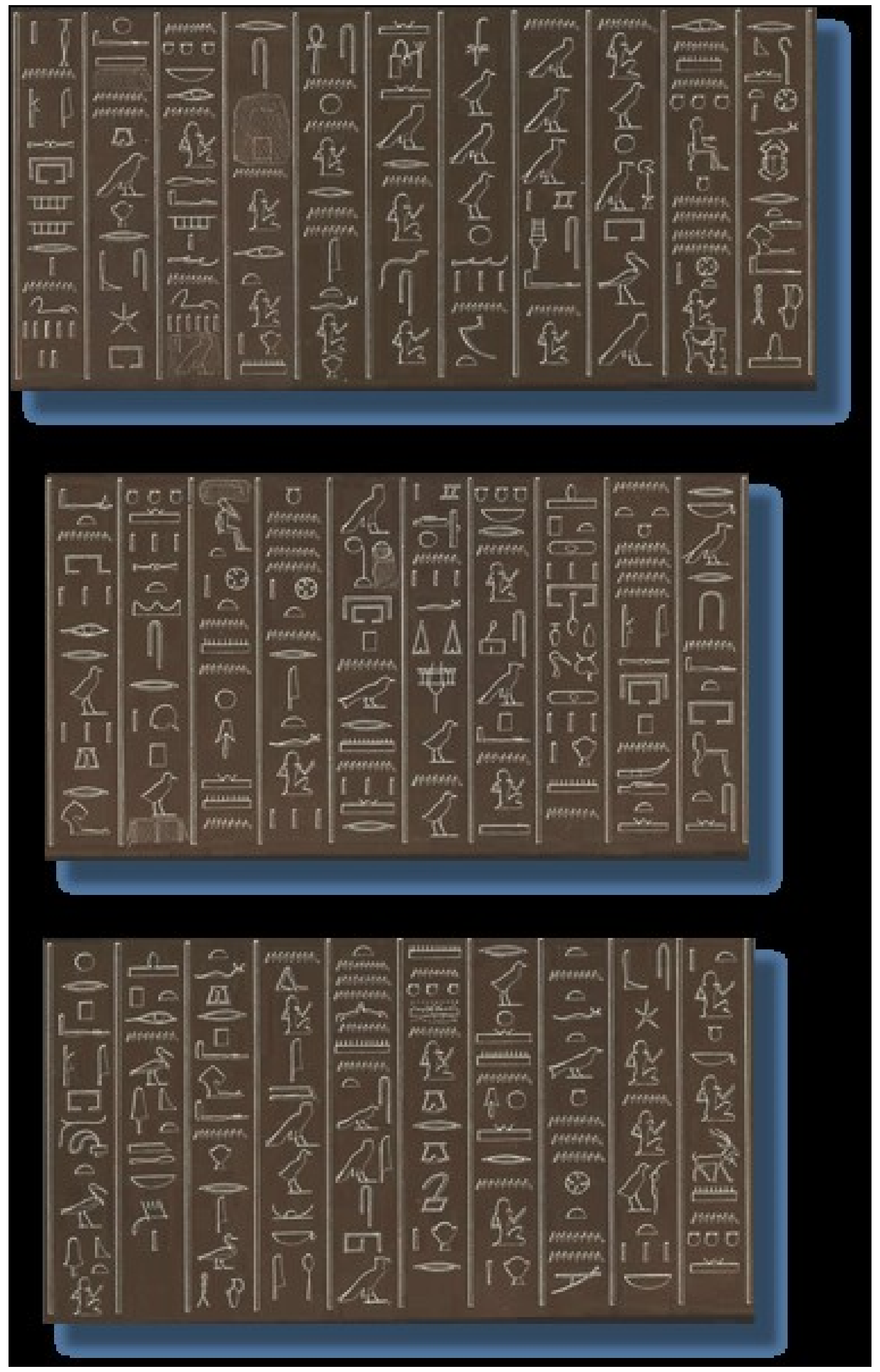
- A quick survey of old cyphers
- Cryptography and diplomacy
- Codes and ciphers
- Cryptography in WWI
- The Zimmerman telegram

Cryptography in history

- Crypto is as old as spies and armies
  - Ötzi, the Alps mummy, was most likely a warrior
  - His tribe certainly has spies and secret messages!

Oldest known ciphertext

- The tomb of Egyptian nobleman Khnumhotep II, buried in 1900 B.C., contains very unusual hieroglyphs.
- The scribe who wrote them used a substitution cypher.
  - Maybe as part of a funeral ritual
  - Or as a “secret prayer” known only to the family
  - Or maybe new trendy religious jargon!



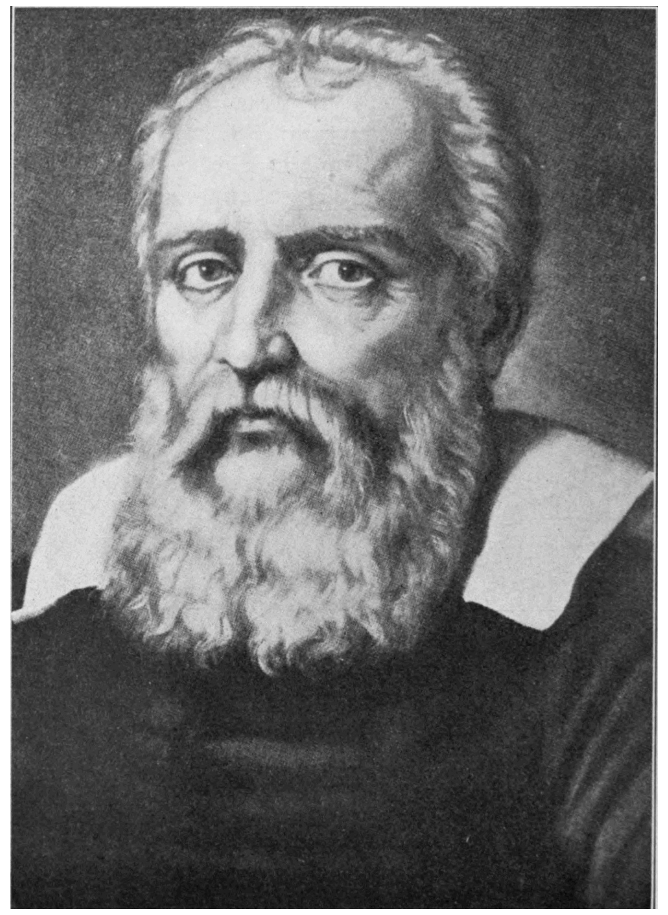
It's not just for spies…

- Some professions used and still use coded writing to keep their secrets
  - Either because of fear of authorities (criminals)
  - Or to keep valuable trade secrets (accountants in ancient Egypt)
  - Or to blame failure on the reader's ignorance (alchemist recipes)
  - Or to taunt rivals (Galileo)

Dear Johannes Kepler,
Are you able to afford a telescope yet?
Look what I found with mine:
smaismrmilmepoetaleumibunenugttauiras
– Galileo Galilei

Dear GG,
Easy. It's an anagram for *Salve umbisteneum geminatum Martia proles* (*), and I already knew that Mars has two moons.
I cannot get a telescope, but I hope you can afford a good lawyer for your libel lawsuit.
- Johannes Kepler

(*)Hail, twin companionship, children of Mars

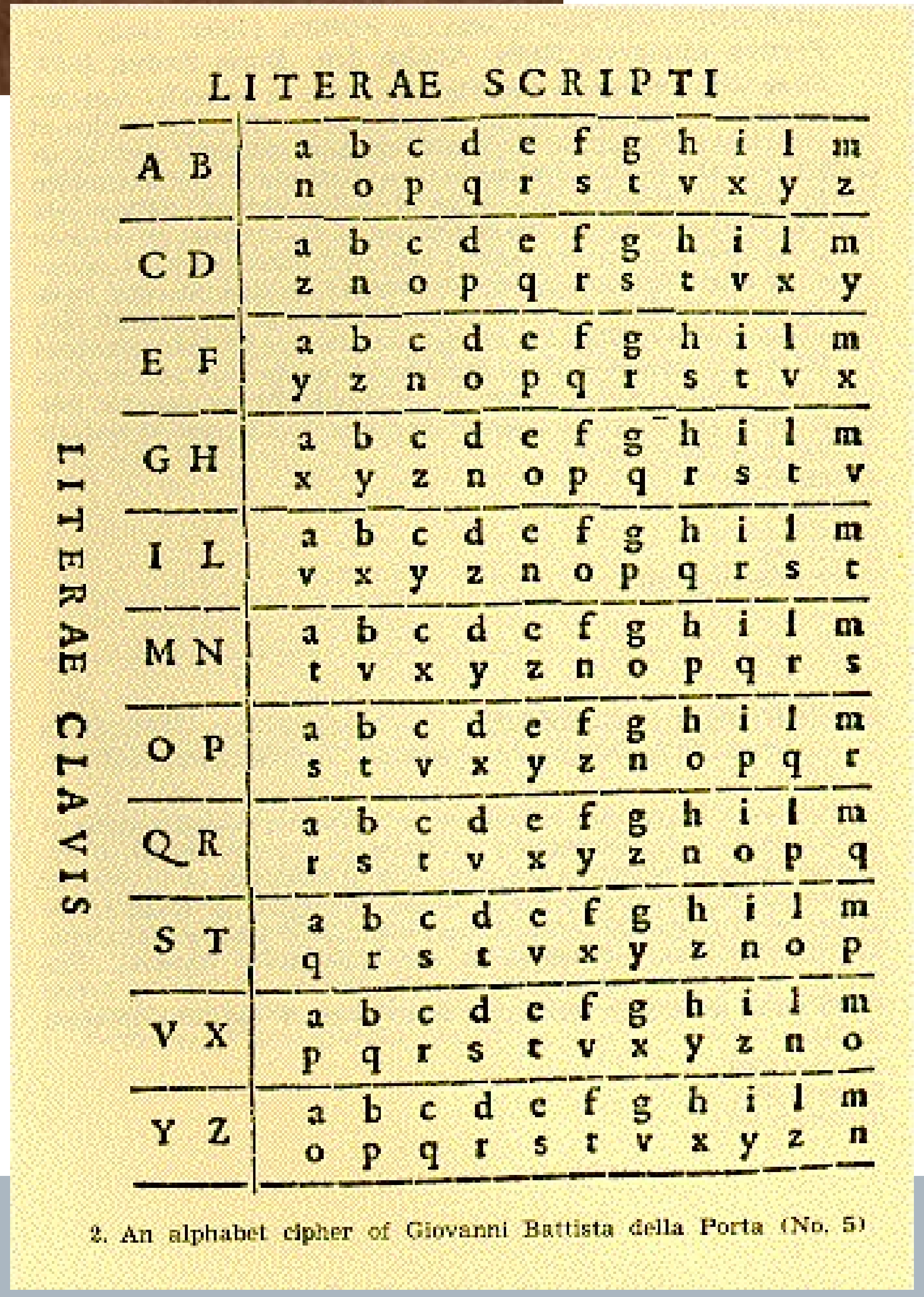


Cryptography and diplomacy

- Diplomats have routinely exchanged secret messages with their home country for thousands of years.
- The message was hidden. Examples:
  - Invisible ink
  - Messages written inside pottery
  - Message written on shaved scalp
- The code was always symmetrical with shared secret.
- Ciphers were almost always substitution.


Copyright 1997 Hirana
ALL RIGHTS RESERVED

A Caesar cipher (50 BC at least)



LITERAE SCRIPTI

LITERAE CLAVIS

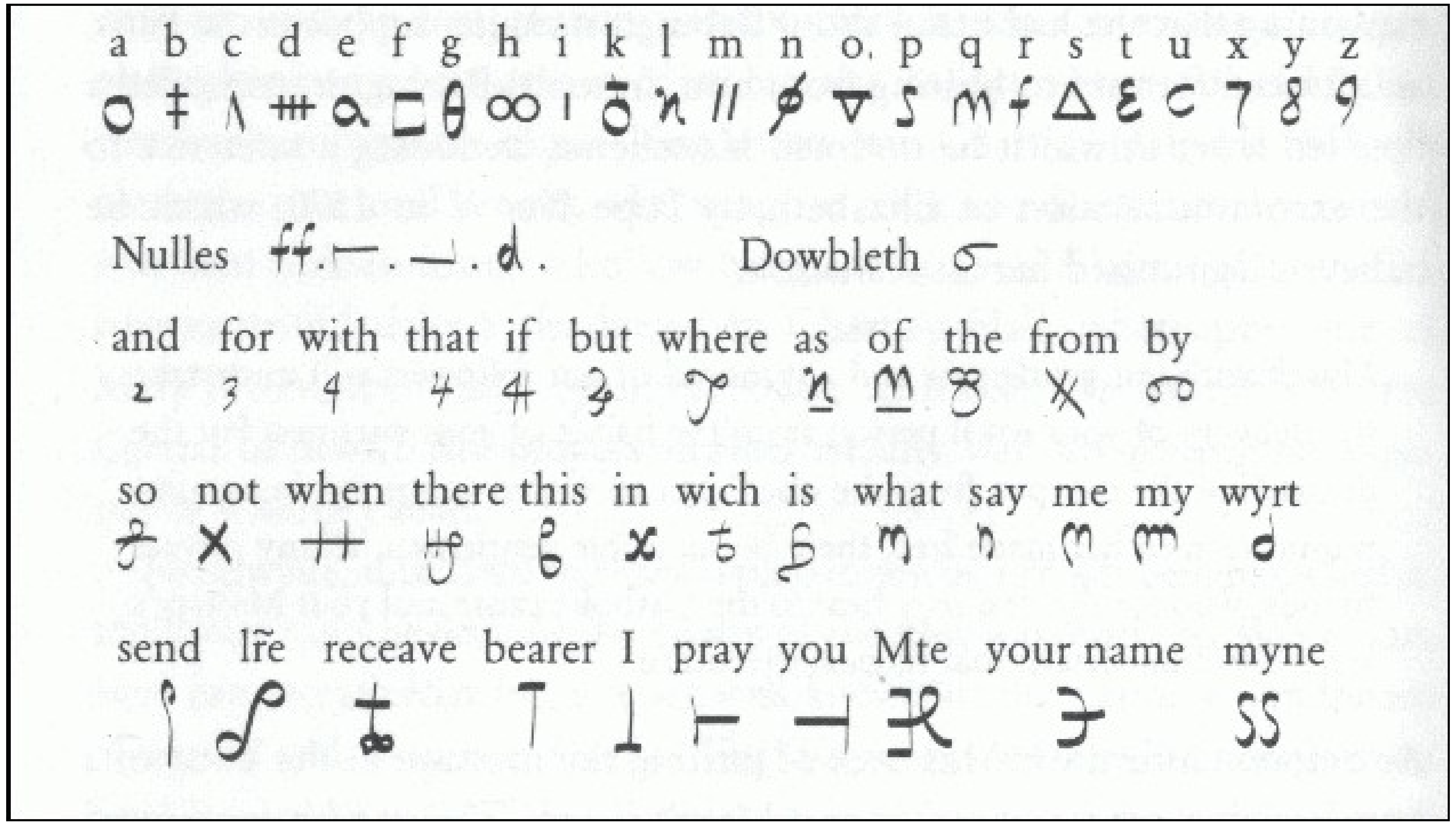
A B	a	b	c	d	e	f	g	h	i	l	m
	n	o	p	q	r	s	t	v	x	y	z
C D	a	b	c	d	e	f	g	h	i	l	m
	z	n	o	p	q	r	s	t	v	x	y
E F	a	b	c	d	e	f	g	h	i	l	m
	y	z	n	o	p	q	r	s	t	v	x
G H	a	b	c	d	e	f	g	h	i	l	m
	x	y	z	n	o	p	q	r	s	t	v
I L	a	b	c	d	e	f	g	h	i	l	m
	v	x	y	z	n	o	p	q	r	s	t
M N	a	b	c	d	e	f	g	h	i	l	m
	t	v	x	y	z	n	o	p	q	r	s
O P	a	b	c	d	e	f	g	h	i	l	m
	s	t	v	x	y	z	n	o	p	q	r
Q R	a	b	c	d	e	f	g	h	i	l	m
	r	s	t	v	x	y	z	n	o	p	q
S T	a	b	c	d	e	f	g	h	i	l	m
	q	r	s	t	v	x	y	z	n	o	p
V X	a	b	c	d	e	f	g	h	i	l	m
	p	q	r	s	t	v	x	y	z	n	o
Y Z	a	b	c	d	e	f	g	h	i	l	m
	o	p	q	r	s	t	v	x	y	z	n

2. An alphabet cipher of Giovanni Battista della Porta (No. 5)

A Porta cipher sheet (16th century)

A famous case: Mary and Elizabeth

- It's not like Alice and Bob: Mary Stuart, Queen of Scots, Mother Queen of France, was imprisoned by her cousin Queen Elizabeth I of England for 18 years.
- In January 1586, she started exchanging crypted messages with Babington, an Englishmen working in France against Elizabeth.
- The messages were substitution-coded, then hidden in wine casks by her friend Gilbert Gifford, who was actually working for Elizabeth's master spy, Francis Walsingham.
- Gifford would deliver the messages to Thomas Phelippes, Walsingham's chief cryptanalyst.
- And thus started the earliest documented man-in-the-middle attack...



a b c d e f g h i k l m n o p q r s t u x y z

Nulles ff. Dowbleth

and for with that if but where as of the from by

so not when there this in wich is what say me my wyrt

send lr̃e receave bearer I pray you Mte your name myne

Mary vs. Elizabeth (cont'd)

- Phelippes decrypted the messages and sent forged copies to Babington.
- When Babington wrote about a plan to assassinate Elizabeth, Mary answered that she approved.
- Phelippes added a post-scriptum to her response asking for the conspirator names.
- Babington obliged. The conspirators were arrested.
- Mary was executed in February 1587.

The Vigenère square

- The first real cryptography breakthrough comes in 1586 from Blaise de Vigenère, a French diplomat posted in Italy.
- The Vigenère square is a variable substitution cipher depending upon one shared secret, the key word.
- The system is hard to break and was used until the 20th century.
- During the American Civil War, the Confederate used a Vigenère code with mostly three pass phrases: "Manchester Bluff", "Complete Victory", and "Come Retribution".
- Babbage developed a (manual) method to crack the code in 1852 but never published it!

```
|---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---|
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
| 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 |
 … and so on...
Keyword: BADBEAD
Plain text: Attack at dawn

Step 1: Remove blanks          ATTACKATDAWN
Step 2: Repeat key as needed   BADBEADBADBE
Result:                        BTWBGKDUDDXR
```

How to use a Vigenère square

Vigenère code during the Civil War

- An example of Confederate message using Vigenère dated July 4, 1863:

Cyphertext: *stan witviivz dtg cnp lbnxok oz bjqb feqt feqt xzbw jjoa tk fhr tpzwk pbw rvsq vowpzxqq oedh ek waskipw plvo jkz hmn nvaeuo xve dwaj boypa sk mlv fyyroelvpl mfysiu xy fqeo npk m obpc fvxjfhoht as etov b ocajosvqu m ztzv tpjy daw fqti wttj j dqgoaia flwhtxti qmtr sta lvlflxfo*

Cleartext:
Gen'l Pemberton:
You can expect no help from this side of the river. Let Gen'l Johnston know, if possible, when you can attack the same point on the enemy's lines. Inform me also and I will endeavor to make a diversion. I have sent some caps . I subjoin a despatch from General Johnston.

Source: http://www.dailymail.co.uk/news/article-1341666/CIA-codebreaker-reveals-147-year-old-Civil-War-message-Confederate-desperation.html

Cryptography during WWI

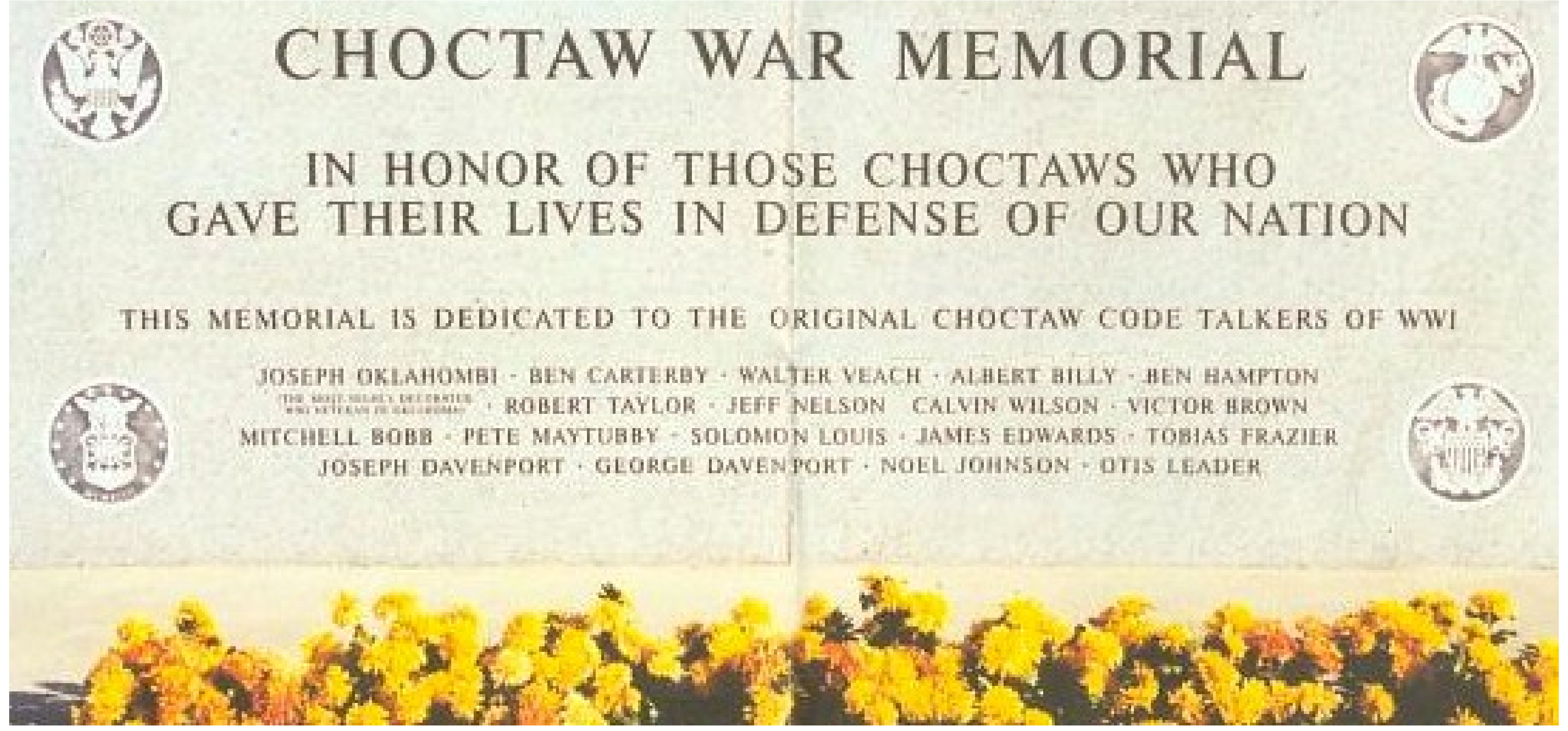
- What changed since the previous conflicts
  - Still no computers – Encoding and decoding messages is largely manual.
  - On the front, coded messages are sent by messengers.
  - The main military message media is the telegraph.
  - Telegrams can be intercepted, although messages going through a country to the front are largely safe, hence lighter encryption for them.
  - Wireless messages obviously need a stronger encryption.
  - Intercontinental radio is still largely experimental. Several cross-Atlantic telegraphic cables are in use.

WWI Trench codes

- The Germans often managed to tap French phone lines even under fire (quite a feat)
- The French developed “trench codes”
  - First an informal mix of *argot* (slang), spelled out words
  - Was later formalized with official codes
  - Complex codes were often judged impractical.
    - Coding was at time sloppy – “communication discipline” problems
    - Incompletely coding a message was worse than no coding at all, since it offered a chance to deduct the coded part, and thus weaken the code.
- The British and German followed with their own systems

American Choctaw code talkers

- When the Americans entered WWI, US cryptography was rudimentary
- In 1918, one Colonel Bloor took Oklahoman Choctaws from his unit and used them as radio and telephone operators.
- Two Choctaws officers set up a training unit for code talkers
- The Choctaws improvised military terms
    - *"Little gun shoot fast", was substituted for machine gun and the battalions were indicated by one, two and three grains of corn.* – Col. Bloor, memo to HQ, Jan 23, 1919



CHOCTAW WAR MEMORIAL

IN HONOR OF THOSE CHOCTAWS WHO
GAVE THEIR LIVES IN DEFENSE OF OUR NATION

THIS MEMORIAL IS DEDICATED TO THE ORIGINAL CHOCTAW CODE TALKERS OF WWI

JOSEPH OKLAHOMBI · BEN CARTERBY · WALTER VEACH · ALBERT BILLY · BEN HAMPTON
· ROBERT TAYLOR · JEFF NELSON CALVIN WILSON · VICTOR BROWN
MITCHELL BOBB · PETE MAYTUBBY · SOLOMON LOUIS · JAMES EDWARDS · TOBIAS FRAZIER
JOSEPH DAVENPORT · GEORGE DAVENPORT · NOEL JOHNSON · OTIS LEADER

An example: The German ADFGVX cipher

- Start with a keyword and a 6x6 square containing all letters and digits. Use ADFGVX as the vertical and horizontal indexes.

	A	D	F	G	V	X
A	p	h	0	q	g	6
D	4	m	e	a	1	y
F	l	2	n	o	f	d
G	x	k	r	3	c	v
V	s	5	z	w	7	b
X	j	9	u	t	i	8

- Encode your message using the square:
  'attack' -> 'DG XG XG DG GV GD'.

- Put the message in columns under each letter of the keyword (here, GERMAN):

G	E	R	M	A	N
D	G	X	G	X	G
D	G	G	V	G	D

- Sort the columns

A	E	G	M	N	R
X	G	D	G	G	X
G	G	D	V	D	G

- The final ciphertext is:

```
XG GG DD GV GD XG
```

Source: http://practicalcryptography.com/ciphers/adfgvx-cipher/

An example: The German ADFGVX cipher

- Start with a keyword and a 6x6 square containing all letters and digits. Use ADFGVX as the vertical and horizontal indexes.

```
    A D F G V X
A | p h 0 q g 6
D | 4 m e a 1 y
F | l 2 n o f d
G | x k r 3 c v
V | s 5 z w 7 b
X | j 9 u t i 8
```

- Encode your message using the square:
  'attack' -> 'DG XG XG DG GV GD'.

- Put the message in columns under each letter of the keyword (here, GERMAN):

```
G E R M A N
- - - - - -
D G X G X G
D G G V G D
```

- Sort the columns

```
A E G M N R
- - - - - -
X G D G G X
G G D V D G
```

- The final ciphertext is:

```
XG GG DD GV GD XG
```

An example: The German ADFGVX cipher

- Start with a keyword and a 6x6 square containing all letters and digits. Use ADFGVX as the vertical and horizontal indexes.

	A	D	F	G	V	X
A	p	h	0	q	g	6
D	4	m	e	a	1	y
F	l	2	n	o	f	d
G	x	k	r	3	c	v
V	s	5	z	w	7	b
X	j	9	u	t	i	8

- Encode your message using the square:
  'attack' -> 'DG XG XG DG GV GD'.

- Put the message in columns under each letter of the keyword (here, GERMAN):

G	E	R	M	A	N
D	G	X	G	X	G
D	G	G	V	G	D

- Sort the columns

A	E	G	M	N	R
X	G	D	G	G	X
G	G	D	V	D	G

- The final ciphertext is:
  `XG GG DD GV GD XG`

- Add other letters of the alphabet to obfuscate

Broken by cryptographer George Painvin in May 1918

Diplomatic codes

- France and Germany had the best mathematicians in the world
- So of course the French and German governments disregarded their work and used substitution and code books.
- Principle:
  - Look up a code book, replace word or syllable with number
  - Optionally, transpose and group the numbers

Diplomatic codes (cont'd)

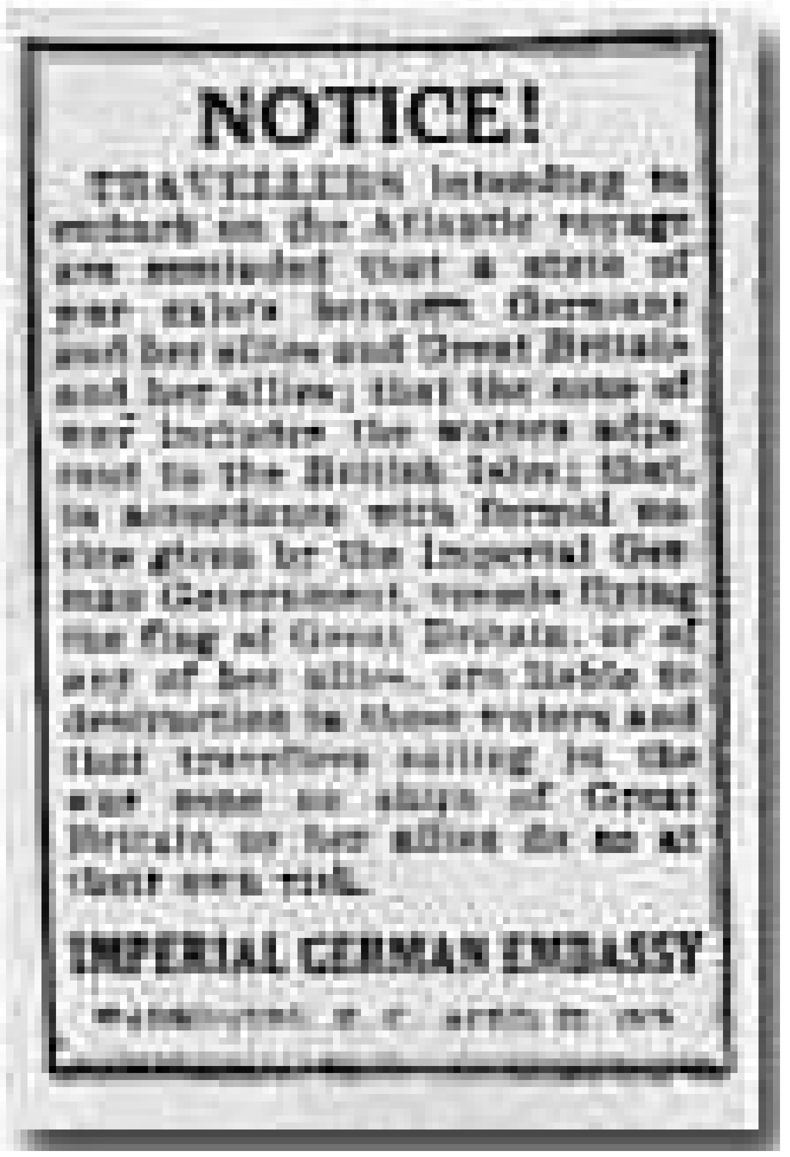
- Some extra obfuscating can be added. Example, the French *Tableau de Correspondance* code:
    - Each word of the cleartext is coded into a 4-digit code
    - Skip the 1st digit.
    - Group the digits in 2-digit pairs.
    - Replace all resulting numbers with two-letter equivalents
- Codes of this type are pretty weak, even without the code books.
    - The Germans reportedly broke the new version of the Russian code in three hours.
    - In 1914, Herbert Yardley, a code clerk at the State Dept., was shocked to find he broke the US code in two hours.

Political situation at the start of 1917

- Woodrow Wilson was reelected on a isolationist platform but he wants to enter the war
  - Officially to help the British
  - As history will show, it's actually because he hates the Austro-Hungarian Empire
- The situation in Europe was deadlocked
  - War of attrition, trenches, deadly offensives on small territories
  - The Germans were losing less people than the French and British, so they were winning.

What about the Lusitania?

- British liner Lusitania was torpedoed in 1915. Why?
  - England was making only a quarter of the explosives it needed
  - The rest was imported, by boat of course.
  - Like every boat sailing to the UK, Lusitania was bringing explosives, unprimed shells and rifle ammo
    - Unrefrigerated crates marked “Oysters” and “Butter” were loaded on board – This was a running joke on the docks.
    - The manifesto lists an impressive tonnage of military supplies
- The Germans warned that if the Brits kept militarizing passenger liners, they will consider them fair targets.
  - The Germans even published warnings in the US press
  - Ironically, some of these were published next to Cunard ads.



NOTICE!
Travellers intending to embark on the Atlantic voyage are reminded that a state of war exists between Germany and her allies and Great Britain and her allies; that the zone of war includes the waters adjacent to the British Isles; that, in accordance with formal notice given by the Imperial German Government, vessels flying the flag of Great Britain, or any of her allies, are liable to destruction in those waters and that travellers sailing in the war zone on ships of Great Britain or her allies do so at their own risk.
IMPERIAL GERMAN EMBASSY WASHINGTON, D.C., APRIL 22, 1915.

Lusitania (cont'd)

- The Germans were attacking any British ship
- Lusitania was torpedoed by U-20 on May 7th, 1915, 12 miles from the Irish coast.
- The single torpedo triggered the explosion of raw explosive stored in the hold, likely gun shell propellant. (Fortunately, the 4 million .303 bullets didn't explode).
- Victims: 1192 out of 1960 aboard died, including 114 Americans.
  - As a result of the outcry, the German Navy toned down its anti-shipping submarine ops for the next 18 months.
  - This triggered anti-German sentiment in the US.
- But in spite of the anger, this could not be a casus belli.

The Zimmermann telegram

- Disclaimer:
  - Even today, the amount of disinformation and propaganda on the subject is unbelievable
  - Some documents were made available only in the late 2000
  - Makes you wonder what BS we are fed about more recent events
- Main source: *The Zimmerman Telegram* by Thomas Boghardt (US Naval Institute Press, 2012.)
  - This book shows rather convincingly that a previous 1985 book of the same title by Barbara W. Tuchman uses sources now known to be untrue.
  - The memoirs of William Hall, head of Room 40 (British cryptography unit), long considered a main source, are a bunch of CYA lies.

The tip of the iceberg

- In January 1917, the German government gave a long coded telegram to the US embassy in Berlin, to be sent to the German embassy in Mexico
- “Personal matters”, they said. “Nothing about the war,” they said.
- The US embassy sent it to Washington through a transatlantic cable passing through the UK.
- The British cryptography office, “Room 40”, routinely intercepted and decoded US diplomatic transmissions.
  - William Hall wanted to hide that fact. Lies upon lies were piled up for 60 years to that effect.
  - The Brits considered the US a fickle an unreliable ally
  - Considering the shock after the NSA German interceptions, Hall was probably justified.

The content of the telegram

- The telegram contained two messages:
  - That unrestricted submarine warfare was going to resume on Feb. 1st to hamper the British supplies. This might bring the US into the war.
  - Two, most importantly: If that doesn't work, make Mexico a proposal to start war against the US to reclaim Texas, New Mexico and Arizona.
  - The German offered to bring gold to Mexico to finance the purchase of weapons.
- Context: The US and Mexico were at war a few years before, and bandit-guerillero Pancho Villa had raided Colombus, NM in 1916 before retreating to Mexico (he needed supplies…)
- Little love between US and Mexico.

The Mexican response

- Wait... You want to give us money to buy weapons from the gringos... To make war against them?
- What, you think they are loco? Why would we need heavy artillery and planes if not to use against them?
- Besides, even if the US matched our troops men-for-men on a southern front, they could still send an expedition to Germany.
- That's the worst idea since jalapeno-infused underpants.

Crypto-diplomacy

- Hall wanted to keep this telegram interception a secret
- He didn't want the US or Germany to change their codes
- He waited until the message had been relayed from Washington to the German embassy in Mexico
- He arranged for a British printer working in the Mexican telegraph office to steal a copy of the telegram
  - The man's brother had been sentenced to death by the Mexican gov't for spying
  - A diplomatic intervention saved him, so the man owed a favor to the British embassy
  - Or at least that's what the official version is.

Crypto-diplomacy (cont'd)

- Hall now had a version that was obtained from an acceptable source. He finally informed his government.
- The British almost immediately told the US government on March 1st
  - At first, the US suspected it was a British hoax to ensnare them into the war
  - Unbelievably, Zimmerman himself confirmed. This is still unclear.
- The outrage gave President Wilson the *casus belli* he wanted, the rest is history.

How did Room 40 break codes?

- According to some sources (including Hall):
    - The Russian recovered a code book from a corpse after the destruction of German light cruiser Magdeburg, and gave it to the British
    - The British found a code book in a U-Boot wreck.
    - A British spy, Alexander Szek, was a telegraph operator in Belgium, and copied the code books. Szek became too jittery and fled to the UK, then Belgium, so Hall said he personally paid £1000 to have him shot (!)
- Boghardt says: All of that is bunk. Room 40 broke the codes through slow, painstaking work using multiple intercepted ciphertexts and trial-and-error methods.
- But the cloak-and-dagger stuff sells better, doesn't it?

Questions?