The Story of the Code Girls

Technical Overview:

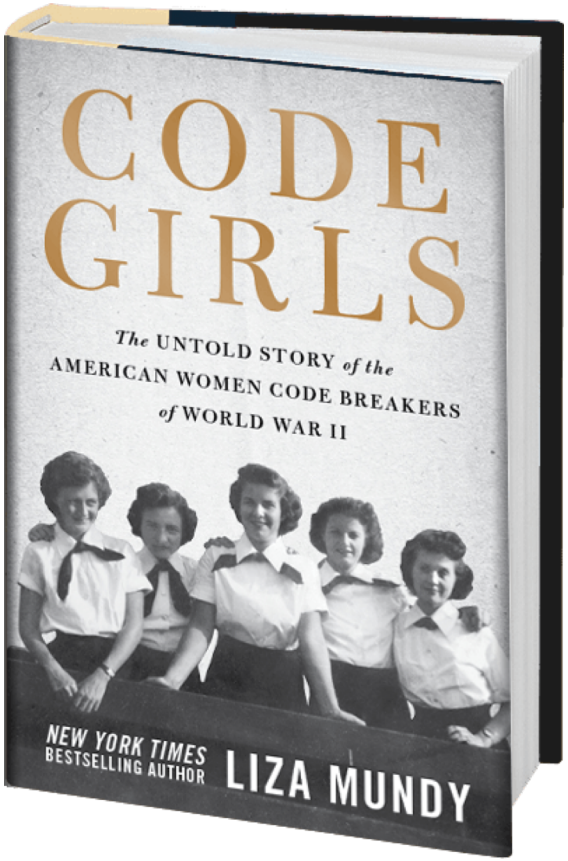
Codes and Ciphers

Cryptanalytic History:

Women in World War II

Put Yourself in the Story:

Working in CA Today



Technical Overview: Ciphers and Codes

Pencil and Paper

- From Antiquity
- Confidentiality
- Technical Highlights
  - Hidden Writing
  - Transposition
  - Substitution
  - CA Methods

Machine Cipher

- Twentieth Century
- Dedicated Cipher Machines
- Mostly Text Only
- Secret Algorithms
- Key exchange by courier
- WWII Technical Highlights
  - SIGSALY
  - JN-25
  - Enigma
  - PURPLE

Public Key Era

- From 1970's and 80's
- Internet and smart devices
- Multi-media encryption
- Known Algorithms
- On-Air Key Exchange
- Technical Highlights:
  - Public Key Exchange
  - RSA & ECC
  - Hash Function
  - Digital Signature
  - AES

Technical Overview: Vocabulary

- **Cryptology** – science of secure communications
- **Cryptographic Functions:**
  - Confidentiality
  - Authentication
  - Integrity
- **Code** – rules and format for representing and sharing information (ASCII, Morse Code, Zip Code)
- **Cipher algorithm** – method to transform information to protect confidentiality, using a secret not shared outside some group
- **Cryptanalysis** – art and science of breaking codes and ciphers *(**CA; Cryptanalyst; Cryppie**)*

Confidentiality: Pencil and Paper Methods

- **Hidden Writing ("low probability of intercept"):**
  - Invisible Ink
  - Shave head, write message on scalp, grow hair
  - Pinpricks in a newspaper or other document
  - Modern examples– steganography, spread spectrum
- **Secret Code** ("code" that is "secret"!) – can be used alone or to prepare input for a cipher system
- **Classic Cipher – Transposition and Substitution**

Secret Code Example: Codebook with two indices

	1	2	3	4	5
A	Girls Talk Math	Meet me	Kirwan	Physics	XFINITY Center
B	Pod Cast	Morning	Afternoon	A	B
C	C	D	E	F	G
D	H	I	J	K	L
E	M	N	O	P	Q
F	R	S	T	U	V
G	W	X	Y	Z	Welcome
H	Crypt	World War II	Code Girls by Liza Mundy	This is very secret info	For your eyes only

`G3 E3 F4` can mix code with `F1 C3 C5 F4 D5 B4 F1` text `G5 F3 E3 H3 A2 A3 B3 H5`

Classic Cipher Vocabulary

Plaintext – the original message

Encipher or ***encrypt*** – change the message to its secret form

Ciphertext – secret form of the plaintext

Decipher or ***decrypt*** – change the ciphertext back to plaintext using the secret key

Break or ***solve*** – determine how to decrypt the ciphertext without knowledge of the secret key

Transposition Cipher – system to rearrange the symbols in the plaintext to produce ciphertext

Substitution Cipher – system to replace each symbol in the plaintext with some other symbol in the ciphertext

Basic Transposition Cipher

- Use an *m* x *n* matrix
- Work in blocks of m*n characters
- Write the plaintext in by rows
- Pull the cipher out by columns

Example Cipher:

```
H9SES SRAAE MG9PE IL9SE

9999M M9YE9
```

Transposition Solution

- Guess that m = 3, n = 10
- To decrypt: write by columns, read plaintext out by rows

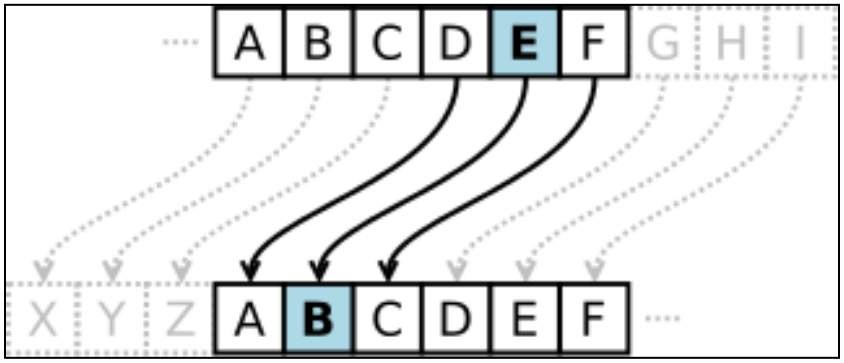
```
H9SES SRAAE MG9PE IL9SE

9999M M9YE9
```

H	E								
9	S								
S									

Simple Substitution Example: Caesar (Shift) Cipher

Each ***plain*** letter is replaced by a ***cipher*** letter that is a fixed ***shift*** away.

Plaintext: ATTACK AT DAWN



Transmitted: XQQXZ HXQAX TL

Math Implementation: ***Modular Arithmetic***

- Represent A-Z by 0-25
- Cipher = Plain + Key
  - If Cipher >= 26 Then Cipher = Cipher – 26
  - If Cipher < 0 Then Cipher = Cipher + 26
- C = (P + K) mod 26
- P = (C – K) mod 26

If you aren't doing the RSA or ECC modules, here is a source on modular arithmetic:
https://en.wikibooks.org/wiki/High_School_Mathematics_Extensions/Primes/Modular_Arithmetic

Caesar Cipher Example

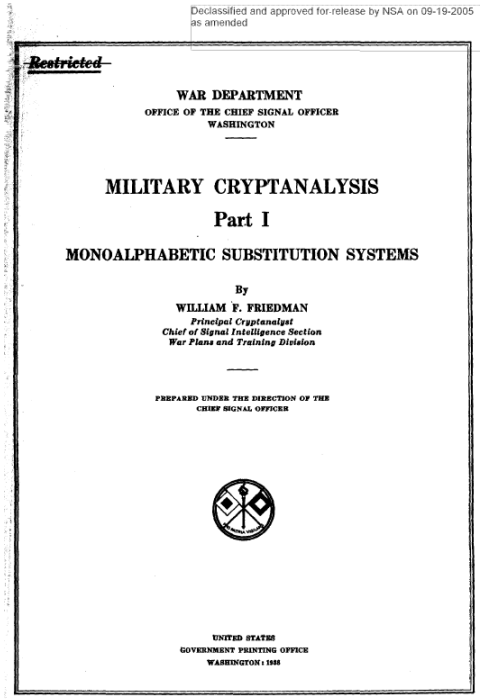
M	A	T	H	I	S	F	U	N
12	0	19	7	8	18	5	20	13
-3	-3	-3	-3	-3	-3	-3	-3	-3
9	23	16	4	5	15	2	17	10
J	X	Q	E	F	P	C	R	K

J	X	Q	E	F	P	C	R	K
9	23	16	4	5	15	2	17	10
3	3	3	3	3	3	3	3	3
12	0	19	7	8	18	5	20	13
M	A	T	H	I	S	F	U	N

For the Caesar cipher, the key (shift) is always 3.
With a repeating sequence of shifts, you get **Vigenère Cipher**

Cryptanalytic Methods

- Exhaustion
- Frequency Matching
- Cribs and Patterns



~~Restricted~~

WAR DEPARTMENT
OFFICE OF THE CHIEF SIGNAL OFFICER
WASHINGTON

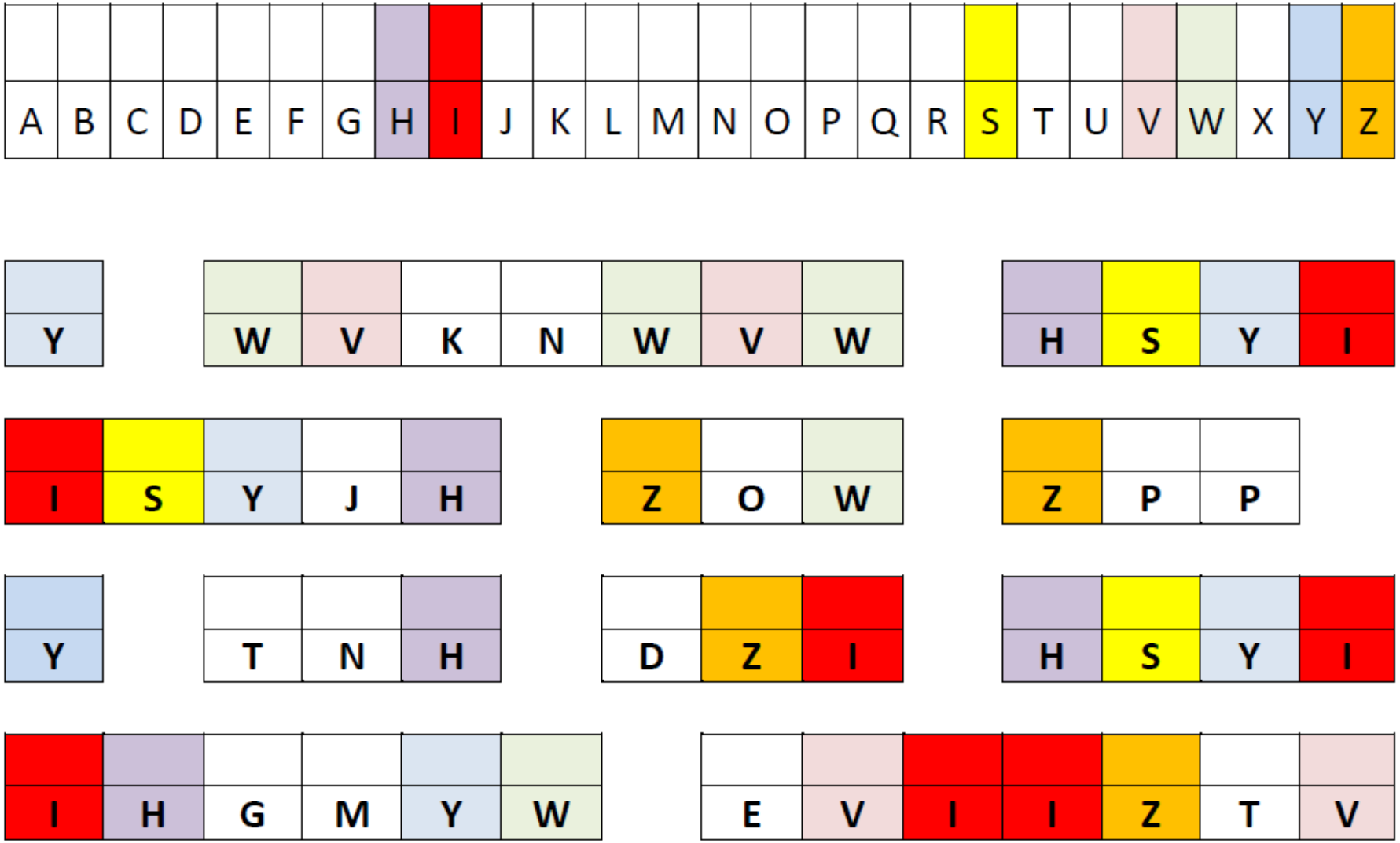
MILITARY CRYPTANALYSIS
Part I
MONOALPHABETIC SUBSTITUTION SYSTEMS

By
WILLIAM F. FRIEDMAN
Principal Cryptanalyst
Chief of Signal Intelligence Section
War Plans and Training Division

PREPARED UNDER THE DIRECTION OF THE
CHIEF SIGNAL OFFICER

UNITED STATES
GOVERNMENT PRINTING OFFICE
WASHINGTON : 1935

First Rule of Cryptanalysis: ***Look at the data. It might be plaintext.***


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
Y
W V K N W V W
H S Y I
I S Y J H
Z O W
Z P P
Y
T N H
D Z I
H S Y I
I H G M Y W
E V I I Z T V

Encrypting Anything: *Digital Stream Cipher*

- Anything on your computer or phone (voice files, videos, music, text files) is represented as many (many) binary digits - 0's and 1's.
- A digital stream cipher uses a key stream of 0's and 1's to encrypt the contents of a file or a communication.
- Each cipher bit is created with mod-2 arithmetic.
  - A logician or a programmer calls this an "exclusive or."
  - An engineer calls this an XOR gate.

cipher = plain ⊕ key

plain = cipher ⊕ key

⊕	0	1
0	0	1
1	1	0

A random key stream that is not re-used is called a one-time pad.

Digital Stream Cipher Example

- Plaintext Message: "A" in ASCII
- **"A" = 01000001**
- **Key = 00101011**
- **$C_i = P_i \oplus K_i$**

Plain	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**1**
Key	**0**	**0**	**1**	**0**	**1**	**0**	**1**	**1**
Cipher	**0**	**1**	**1**	**0**	**1**	**0**	**1**	**0**

To be fully modern you could also permute the cipher bits.

Technical Overview: Ciphers and Codes

Pencil and Paper

- Dating from Antiquity
- Confidentiality
- Technical Highlights
  - Hidden Writing
  - Substitution
  - Transposition
  - CA Methods

Machine Cipher

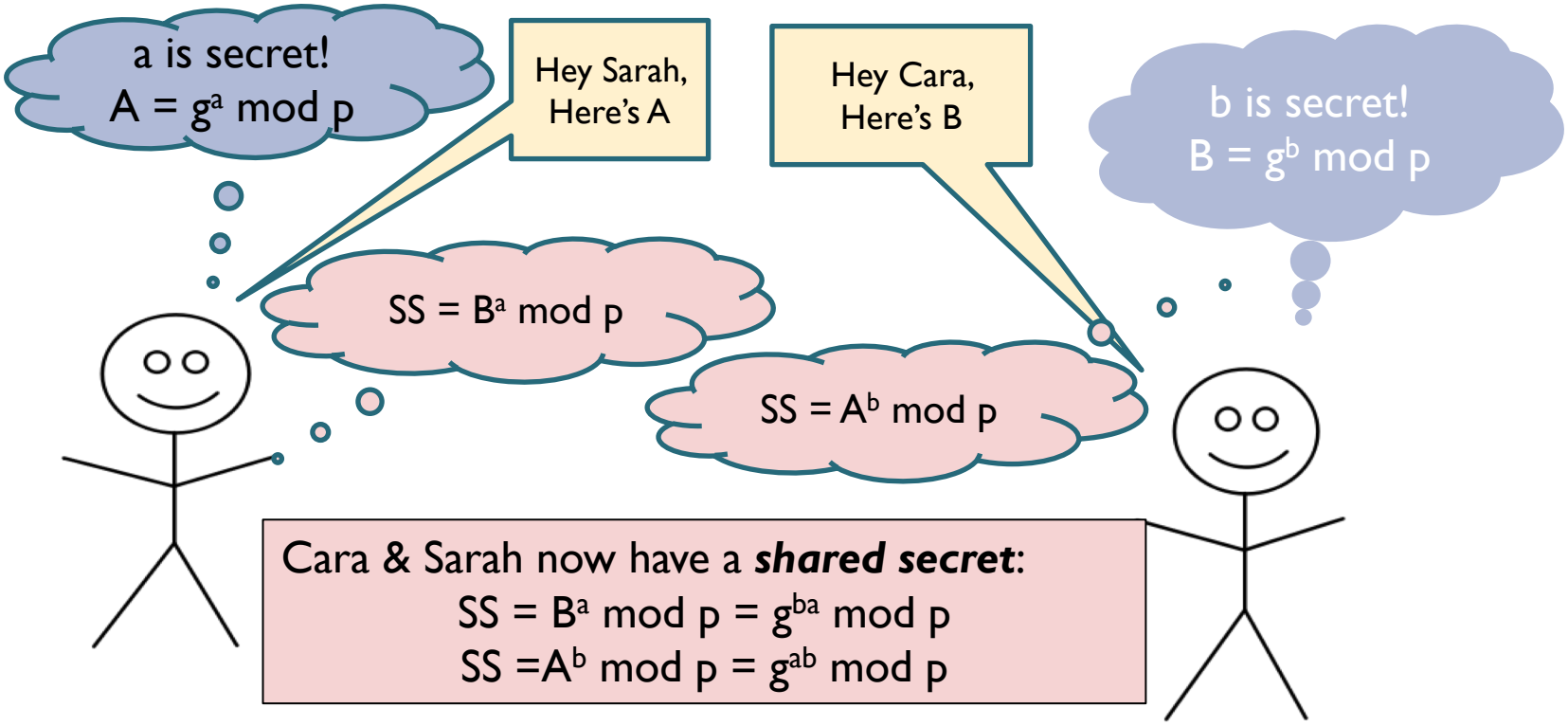
- Twentieth Century
- Dedicated Cipher Machines
- Mostly Text Only
- Secret Algorithms
- Key exchange by courier
- WWII Technical Highlights
  - SIGSALY
  - JN-25
  - Enigma
  - PURPLE

Public Key Era

- Dating from 1970's and 80's
- Internet and smart devices
- Multi-media encryption
- Known Algorithms
- On-Air Key Exchange
- Technical Highlights:
  - Public Key Exchange
  - RSA & ECC
  - Hash Function
  - Digital Signature
  - AES

Public Key Exchange

Diffie-Helman Key Exchange: Public Primes g and p



Sample Calculation
g = 11 and p = 23

- **Cara: a = 3, Sarah: b = 6**
  - $A = 11^3 \bmod 23 = 20$
  - $B = 11^6 \bmod 23 = 9$
  - $A^b \bmod p = 20^6 \bmod 23 = 16$
  - $B^a \bmod p = 9^3 \bmod 23 = 16$
- **Eavesdropper Eve**
  - Calculates a discrete log lookup table
  - Intercepts A and B
  - $a = \log_{11} 20 \bmod 23 = 3$
  - $b = \log_{11} 9 \bmod 23 = 6$
  - Shared secret = $11^{6(3)} = 11^{18} = 16$
  - Only feasible for small p and g

x	g^x
1	11
2	6
3	20
4	13
5	5
6	9
7	7
8	8
9	19
10	2
11	22
12	12
13	17
14	3
15	10
16	18
17	14
18	16
19	15
20	4
21	21
22	1

y	log
1	22
2	10
3	14
4	20
5	5
6	2
7	7
8	8
9	6
10	15
11	1
12	12
13	4
14	17
15	19
16	18
17	13
18	16
19	9
20	3
21	21
22	11

Security: solving the discrete log problem is infeasibly hard for large g and p, equivalent in complexity to factoring their product

g^a with REALLY BIG numbers

- **With large g and p**, calculating g^a and g^b directly causes **overflow errors**
- **One solution:** multiply (and mod) to get $g, g^2, g^3, g^4, \ldots, g^a$
- **When a is a power of 2: use repeated squaring**
  - Example: a = 64
  - Start with g^1 mod p
  - Square (and mod) to get $g^1, g^2, g^4, g^8, g^{16}, g^{32}, g^{64}$
- **In general: look at the binary representation**
  - Example: a = 11
  - 11 = 8 + 2 + 1
  - Square (and mod) to get g^1, g^2, g^4, g^8
  - Multiply (and mod) to calculate $g^{11} = g^1 g^2 g^8$
- **Built into python**: g^a mod p = pow(g,a,p)

Elliptic Curve Public Key Exchange

- Another way to find a shared secret value uses
  - Elliptic curve E: $y^2 = x^3 + ax + b$
  - Finite field F
  - Point G on the Curve E(F)
  - *Note: the points on the curve form a group*
- In the Elliptic Curve module you will learn:
  - What all these terms mean!
  - How to add points P and Q on the curve E(F) with the group law
  - How to find aP = $\underbrace{P + P + P + P \ldots + P}_{a \text{ times}}$
- Shared secret calculation:
  - Cara picks a number a and publishes A = aG
  - Sarah picks a number b and publishes B = bG
  - Shared secret = bA = aB = abG
- Security again depends on the discrete log problem

Cryptographic Hash

- One-way function that maps an arbitrary string of data into a fixed-length ***hash*** value
- Important Properties
  - Quick to compute
  - Infeasibly hard to go backwards
  - Small change of input can lead to a large change in the output
  - Likelihood of a collision is vanishingly small
- Cryptographic Uses
  - Data Integrity and check for updates
  - Authentication
  - Technical (but not legal) non-repudiation

RSA(*) Encryption: How does it work?

- Cara's Public key: (N = 323, e = 11)
- Cara's Secret key: d = 131
- Sarah's wants to send m = 21 to Cara

Sarah sends:

Cipher = $m^e \bmod N$

Cipher = $21^{11} \bmod 323 = 319$

Cara decrypts:

Plain = $(m^e \bmod N)^d \bmod N$

Plain = $319^{131} \bmod 323 = 21$

(*) RSA:
Ron Rivest,
Adi Shamir
Leonard Adleman

RSA Part 2:
Where do N, d and e come from?

- Take two prime numbers p and q
  - For our example take p = 17, q = 19
- Calculate N = p*q and $\varphi(N) = (p-1)(q-1)$
  - N = 17 * 19 = 323
  - $\varphi(N) = 16 * 18 = 288$
- Now choose our public exponent e
  - For our example take e = 11
- Now calculate d so that $d * e \equiv 1 \pmod{\varphi}$
  - In our example, d = 131

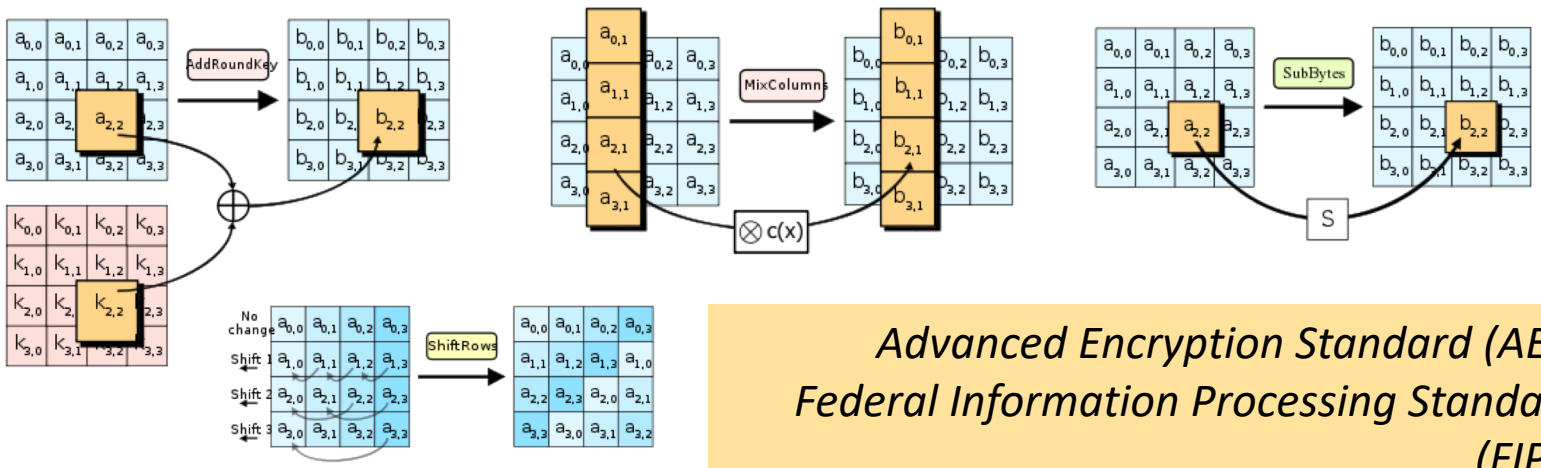
The RSA Math Magic: $a^{\varphi(N)} \equiv a \bmod N$

RSA Part 3: Why does it work?

- **Remember the RSA parameters:**
  - N = p*q for two large primes p and q
  - d*e ≡ 1 mod $\varphi(N)$, where φ(N)= (p-1)(q-1)
  - N and e are public
  - d, p, q and φ(N) are all kept secret
- **Fun math fact from the RSA module:**
  - If d*e≡ 1 mod $\varphi(N)$, then m^{de} mod N = m
- **As a result**
  - When d is known, decryption is fast
  - If d is unknown, decryption requires factoring N
  - With good parameters, this is infeasible

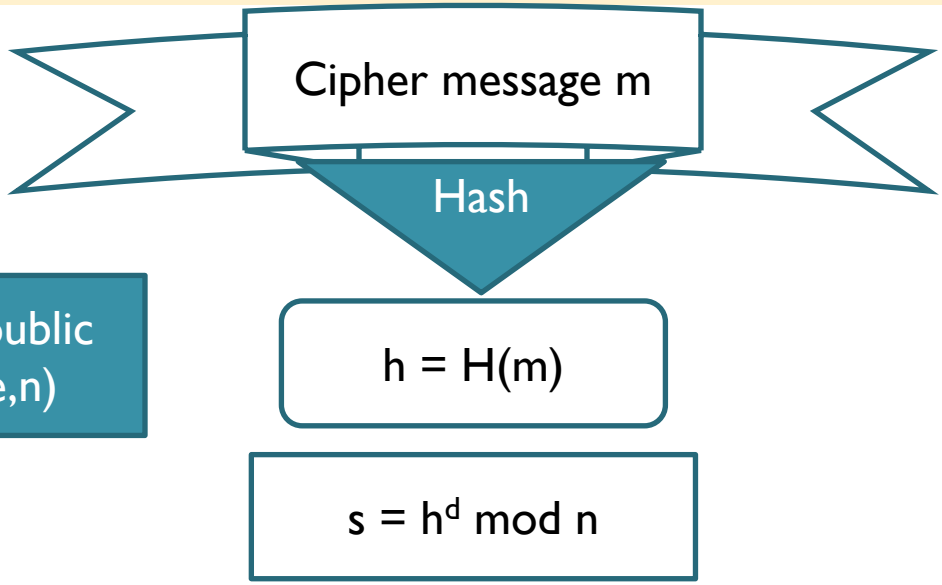
Encryption by Acronym: AES, FIPS 197, NIST 2001(*)

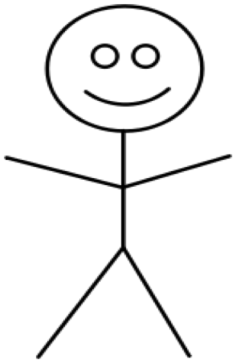
- AES encrypts in blocks of 128 bits
- Multiple rounds of 'substitution' and 'transposition' are used on the bits
- Approved for Top Secret information



Advanced Encryption Standard (AES)
Federal Information Processing Standard (FIPS)
National Institute of Standards and

Cryptographic Signature

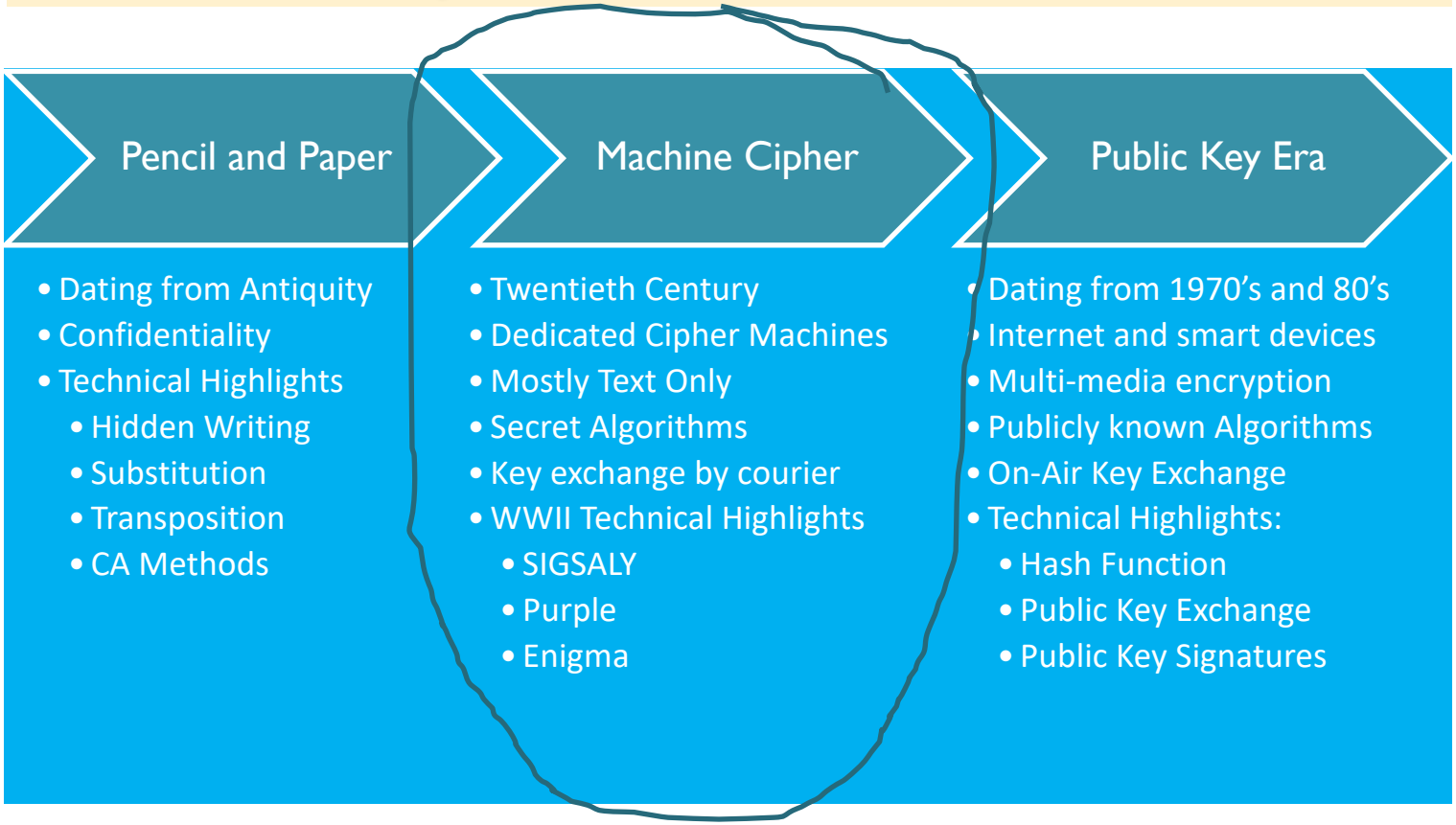




Sarah thinks: Someone sent me *m* and *s*.

- I know Cara's public key is (*e*,*n*).
- I compute *h* = H(*m*).
- I compute s^e mod n. By RSA, this should be h.
- If it matches h, only Cara could have signed it.
- Because only Cara knows her private key *d*.

Technical Overview: Ciphers and Codes



SIGSALY: U.S. Voice

First secure voice for telephones

- Built by Bell Laboratories in 1943
- 55 tons, 40 racks of equipment
- 13 people to operate, 15 minutes to set up each call
- Encrypted with records of random noise
- Used by Roosevelt and Churchill in WWII
- Never broken – Germans thought it was static

JN-25: Japanese Codebook

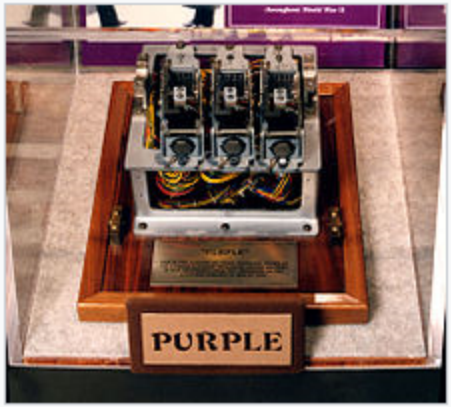
- Approximately 27,500 entries
- Additive book for super-encipherment
  - 300 pages, 100 5-digit groups per page
  - Added without a "carry"
- Cryptanalytic challenges
  - Recover the indicator in each message
  - Recover and strip away additives
  - Recover the code group meanings in Japanese

Enigma: German cipher machine

- Polyalphabetic Substitution
  - Operator types plain character
  - Electrical circuit created
  - Cipher character lights up
  - Rotors move to a new position
- Message settings
  - Plug board with 0-13 cables
  - Selection and ordering of 3 wired rotor discs
  - Initial rotation of the wired discs
- Theoretical configurations: 2×10^{145}
- Configurations as operated: 1×10^{23}
- Portable and widely used by German military

Codename PURPLE: Japanese Cipher Machine

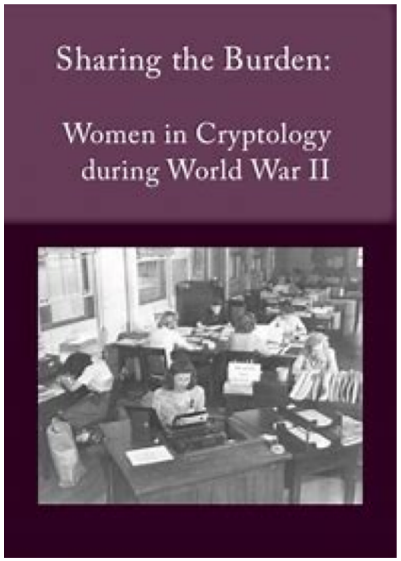
- Similar to Enigma In Operation
  - Typewrite input
  - English, romaji and Roman
  - 4 electric coding rings
  - Stepping switches instead of rotors
  - Output printer unit instead of lights
- Configurations: 1×10^{13}
- Too heavy to be field deployable
- Japanese diplomatic traffic



Fragment of a Type 97 "Purple" cipher machine reverse engineered by the United States Army from the Japanese embassy in Berlin at the end of World War II.

Code Girls: American Women Codebreakers

- Context: Situation upon US entry to WW II
  - Background: European Successes on Enigma
  - State of United States Intelligence
  - United States Society
  - Attitudes to War
- Code Girls:
  - Recruitment
  - By the Numbers
  - Code Girl Culture
- War Effort
- Hall of Honor Cryptanalysts



European Successes on Enigma

- **1926: Germans start to use Enigma**
- **1931: Secret Enigma plans sold to France then given to Polish Cipher Bureau**
  - Bureau include mathematicians in addition to traditional language experts
  - Polish crypto-mathematician spends a year analyzing message features
  - First to employ higher-algebraic attack against any cryptographic system
  - Designs and builds the Bomba, a way to solve and decrypt messages
- **December 1938: Germany upgrades Enigma**
- **July 1939: fearing invasion, Poland reveals details of their success on Enigma to France and Britain**
- **Invasion comes on September 1, 1939**
- **1939-1940:** Alan Turing and Gordon Welchman design the bombe, an electro-mechanical device used to break Enigma messages
- **February 1942: German U-Boats upgraded to 4-rotor machines**

US Intelligence prior to Pearl Harbor

United States Cryptologic History, Series IV, World War II, by Robert L. Benson

- **US intelligence resources limited overall:**
  - Fledgling Intelligence Service – newly formed Coordinator of Information
  - Modest counter-intelligence capabilities
  - Navy and Army dependent on attaches and observers overseas
  - A few women were already serving as cryptanalysts in the military
- **Communications Intelligence (COMINT)**
  - U.S. Army: 331 people at the Signals Intelligence Service
  - U.S. Navy: 730 people at communications security section (OP-20-G)
  - U.S. Coast Guard: Elizebeth Friedman was Chief Cryptanalyst; as an extension of finding rumrunners, also identified clandestine German stations operating in the Western Hemisphere
- **COMINT Cooperation with the British: "fact of US policy"**
  - January 1941: US shares information on PURPLE; Britain shares information on ENIGMA
  - February 1941: US releases a Japanese merchant ship code, a naval personnel code, and callsign information to the British; Britain provides information on JN-25, the most valuable Japanese Naval system for COMINT

United States Society before WW II

- Women have limited access to higher education
  - Caps on admission
  - Families paid for sons, not daughters
  - Few or no spots in graduate school
  - At the elite women's colleges, expectation and strong pressure to marry
- Few jobs for educated women
- Bar on married women in many of those professions, including school teacher
- Washington D.C. is a segregated city

Attitudes to War

- 2018: Is the US at war today?
  - Do you know someone in the military? Someone deployed?
- 1968: Viet Nam is at its height.
  - Draft evaders have been emigrating to Canada.
  - Walter Cronkite calls for an end to the war on CBS news.
- 1938: the world is on the verge of war.
  - September 1, 1939 Germany invades Poland.
  - September 3, 1939 France and Britain declare war on Germany.
- December 7, 1941 – Japan attacks Pearl Harbor
  - Congress declares war on Japan and then on Germany
  - Fear of further attack promotes patriotism & a spirit of sacrifice
  - On the home-front, rationing and victory gardens
  - As tens of thousands of men go to war, women take over many roles formerly reserved for men.

Code Girls: Recruitment

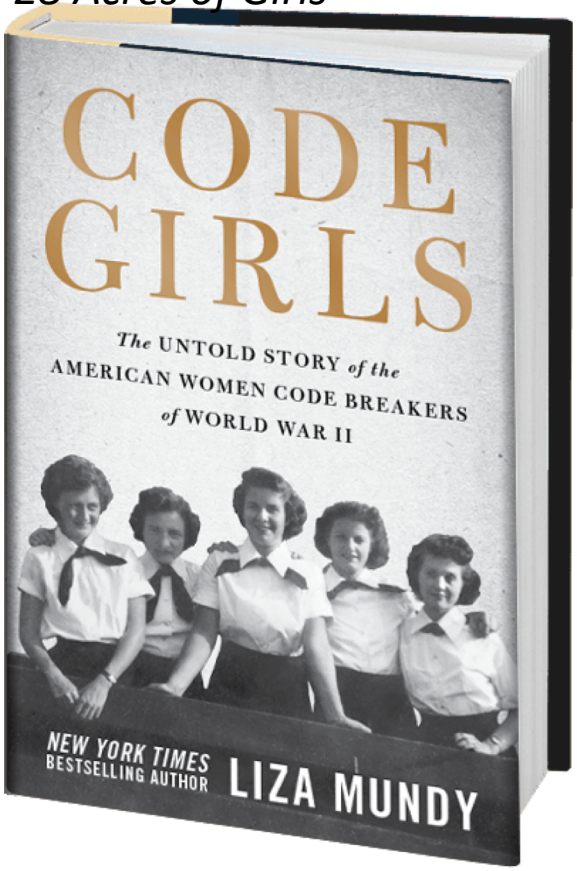
- **U.S. Navy**
  - Secret recruitment at elite women's colleges
  - Recruits chosen for academics, character, loyalty and grit
  - Only two Interview questions:
    - *Are you engaged to be married?*
    - *Do you like crossword puzzles?*
  - By June 1942 – first trainees report to Washington D.C. as Navy civilians
- **U.S. Army**
  - By April 1942, the Army also recruiting women as cryptanalysts
  - Navy brass objected to them "cutting in" at the elite women's colleges. So instead….
    - Teaching colleges throughout the South and Midwest
    - Female school teachers

Code Girls by the Numbers:
over half of all US WW II code-breakers

- 1945 Army code-breakers
  - 8000 working at Arlington Hall
  - 2500 serving in the field
  - 70% female overall
- 1945 Navy code-breakers
  - 5000 working in Washington D.C.
  - 80% female in Washington
  - About 40% female overall

Code Girls Culture

In Washington, Arlington Farms was fast becoming known as Girl Town. " 28 Acres of Girls"



All the girls were writing letters, often to lots of soldiers, and many women received three or four or five letters a day.

It was a profound situation, psychologically. The women were brought in to free men to go forth and, potentially, die. Yet the work they were doing was intended to ensure that those men lived.

Codes are broken not by solitary individuals but by groups of people trading pieces of thing they have noticed, learned and collected.

It was a rare moment in American history - unprecedented - when educated women were not only wanted but competed for.

Code Girl Gallery

Japanese Foreign Ministry: RED and PURPLE Machines

- **Japanese Foreign Ministry Cipher Machines**
  - 1935 –starts using a cipher machine code-named RED
  - February 1937 – SIS produces first RED translation
  - March 1939 – Foreign Ministry starts using PURPLE
- **RED and PURPLE in use simultaneously**
  - Both Split encryption 6/20 (based on earlier coded cable constraints)
  - SIS uses cribs from RED messages and solves the PURPLE "sixes"
  - But progress is slow on the "twenties"
  - Meanwhile, both the British and the U.S. Navy have given up on PURPLE as too difficult
- **September 20, 1940 – Genevieve Grotjan breaks the twenties and completes the solution of PURPLE**
- **William Friedman on PURPLE:**
  - "By far the most difficult cryptanalytic problem successfully handled and solved by any signal intelligence organization in the world."
  - "The most important source of strategically valuable, long-term intelligence."

German U-Boats and Enigma

- February 1942: Enigma machines on U-boats upgraded to four rotors
- *Bombes* at Bletchley Park can no longer read traffic critical to the Battle of the Atlantic
- March 1942:
  - U.S. Navy contracts with National Cash Register Company (NCR) in Dayton Ohio
  - Naval Computing Machine Laboratory (NCML)
  - Public knowledge – NCML builds bomb fuses, shell casings and the like
  - Secret – research to prepare for building a U.S. version of the Bombe to work on four rotors

Enigma and the *WAVES

- **April 1943: Navy personnel come to NCR in Dayton**
  - Eventually 200 sailors and 600 WAVES
  - Cover story: training on tabulating machines
  - Reality: Tedious, tiring work to solder the rotor
- **May 1943: Adam & Eve**
  - First two prototype U.S. Bombes
  - Got a hit on first trial run
    - Cryptanalysts in D.C. broke a U-boat message
    - Allies sunk the U-Boat and 3 submarines
- **Washington: WAVES run the Bombes**
  - By end of 1943, 77 Bombes in operation
  - Eventual total of 120 Bombes built and installed
  - 4 operators and a supervisor for each machine
  - Routinely break U-boat messages
  - Typical time to break U-Boat daily key: 12 hours

(*) Women Accepted for Voluntary Emergency Service

Each Bombe:

5,000 pounds
7 feet high
2 feet wide
10 feet long

NSA Hall of Honor Members

- Elizebeth Smith Friedman
- Agnes Myer Driscoll
- Juanita Moody
- Genevieve Grotjan Feinstein
- Ann Caracristi

Exhibit Gallery

Put Yourself in the Story: Yesterday, Today, Tomorrow

NSA Careers

NSA | CSS National Security Agency | Central Security Service
Defending our Nation. Securing the Future.