Dec 2024

Cryptography & Pacific War

Felix Wu

Pingxiang Middle School

Table of Contents

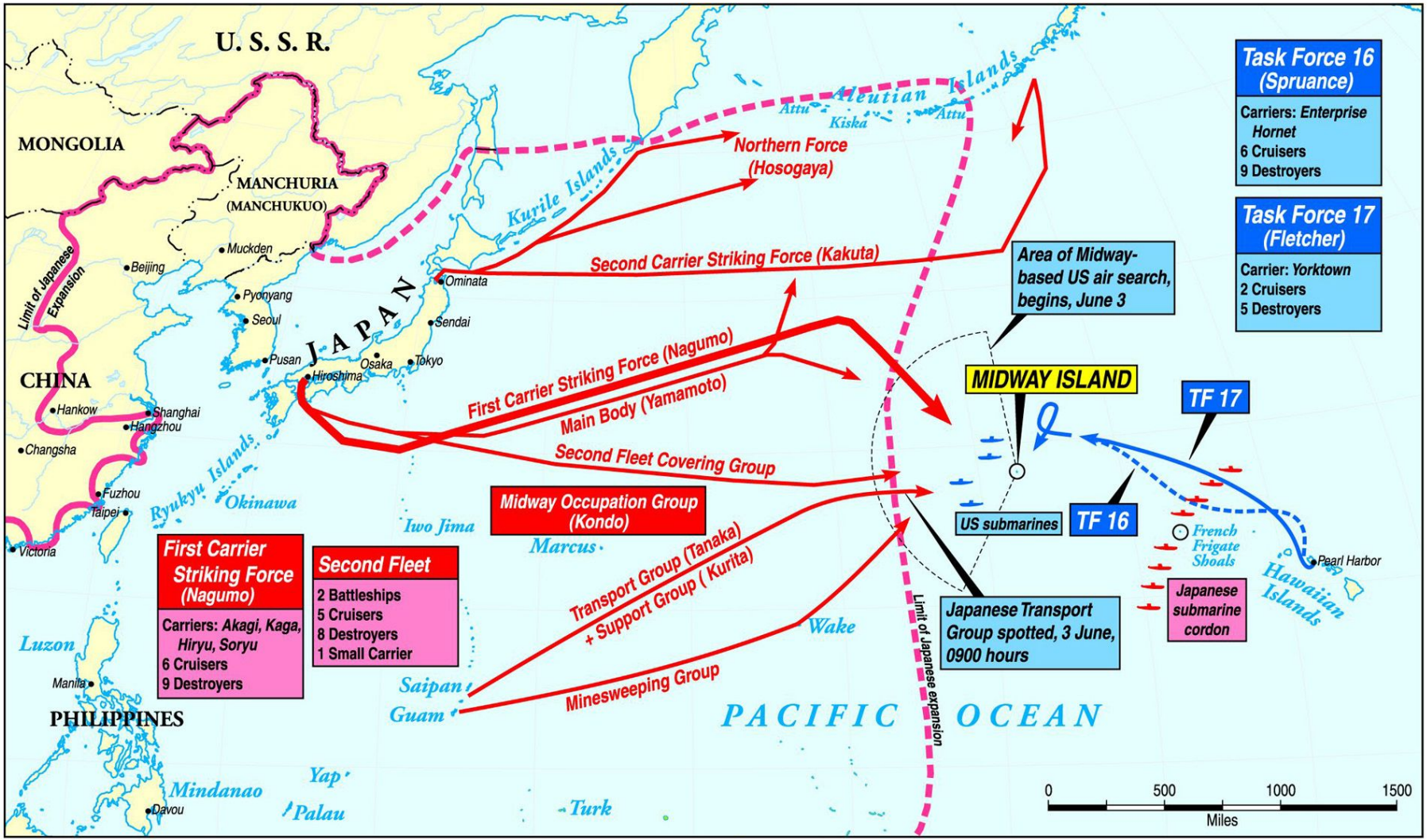

ED SKREIN
PATRICK WILSON
LUKE EVANS
AARON ECKHART
NICK JONAS
WITH MANDY MOORE
WITH DENNIS QUAID
AND WOODY HARRELSON
FROM THE DIRECTOR OF
INDEPENDENCE DAY
MIDWAY
BASED ON REAL EVENTS

Richard Halsey Best

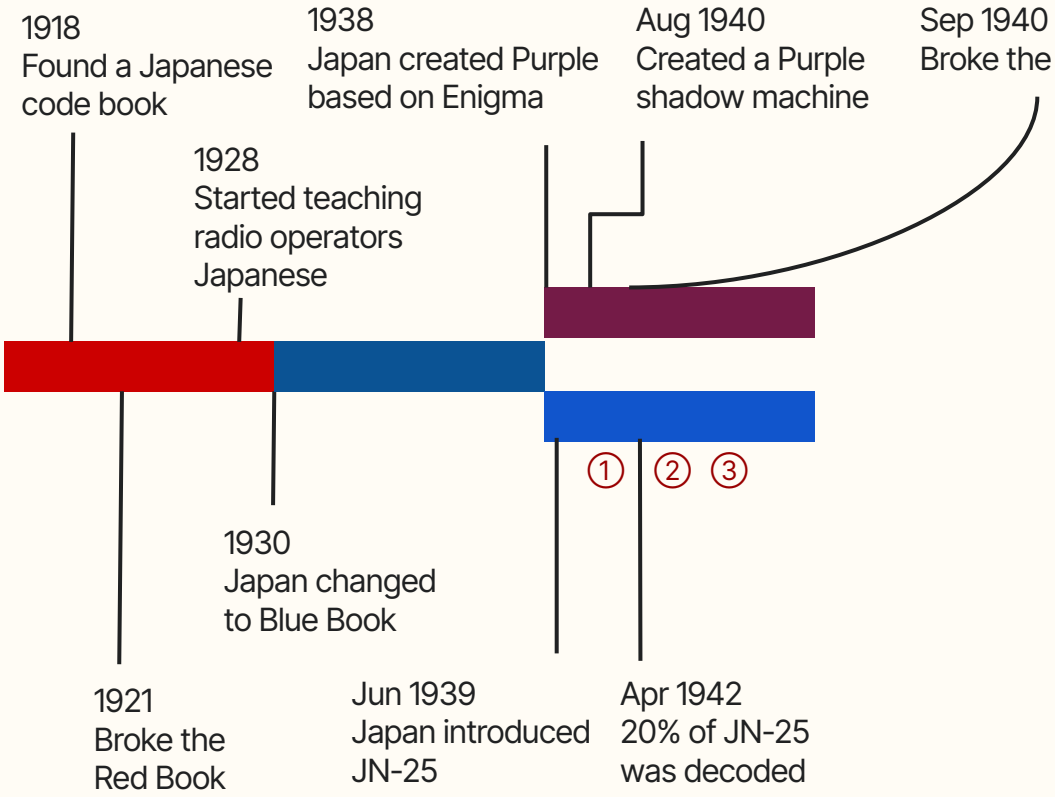
The only pilot who has sunk two aircraft carriers (赤城 / 飛龍) in a single day.

Navy Cross:	August 7, 1942
Service:	United States Navy
Rank:	Lieutenant Commander
Battalion:	Bombing Squadron 6 (VB-6)
Division:	U.S.S. Enterprise (CV-6)
Action Date:	June 4 – 6, 1942

Q: Can you name any other famous heroes in the Pacific War?


U. S. S. R.
MONGOLIA
MANCHURIA
(MANCHUKUO)
CHINA
JAPAN
PHILIPPINES
PACIFIC OCEAN
Limit of Japanese Expansion
Muckden
Beijing
Pyonyang
Seoul
Pusan
Ominata
Sendai
Osaka
Tokyo
Hiroshima
Hankow
Shanghai
Hangzhou
Changsha
Fuzhou
Taipei
Victoria
Luzon
Manila
Mindanao
Davou
Yap
Palau
Turk
Saipan
Guam
Wake
Marcus
Iwo Jima
Okinawa
Ryukyu Islands
Kurile Islands
Aleutian Islands
Attu
Kiska
Attu
Northern Force (Hosogaya)
Second Carrier Striking Force (Kakuta)
First Carrier Striking Force (Nagumo)
Main Body (Yamamoto)
Second Fleet Covering Group
Midway Occupation Group (Kondo)
Transport Group (Tanaka) + Support Group (Kurita)
Minesweeping Group
Area of Midway-based US air search, begins, June 3
MIDWAY ISLAND
US submarines
TF 17
TF 16
French Frigate Shoals
Japanese submarine cordon
Pearl Harbor
Hawaiian Islands
Japanese Transport Group spotted, 3 June, 0900 hours
Limit of Japanese expansion
Task Force 16 (Spruance)
Carriers: Enterprise
Hornet
6 Cruisers
9 Destroyers
Task Force 17 (Fletcher)
Carrier: Yorktown
2 Cruisers
5 Destroyers
First Carrier Striking Force (Nagumo)
Carriers: Akagi, Kaga, Hiryu, Soryu
6 Cruisers
9 Destroyers
Second Fleet
2 Battleships
5 Cruisers
8 Destroyers
1 Small Carrier
0
500
1000
1500
Miles

Why did the US Navy Ambush there?

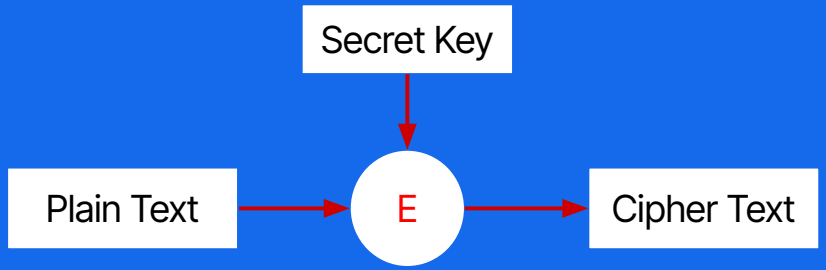


①	Dec 7 1941	Attack on Pearl Harbor
②	May 27 1942 Jun 4-6 1942	AF is short of water Battle of Midway
③	Apr 18 1943	Operation Vengeance

What is Cryptography?

Cryptography is the process of hiding or coding information so that only the person a message was intended for can read it. It's part of Secure Communication.

Encryption & Decryption

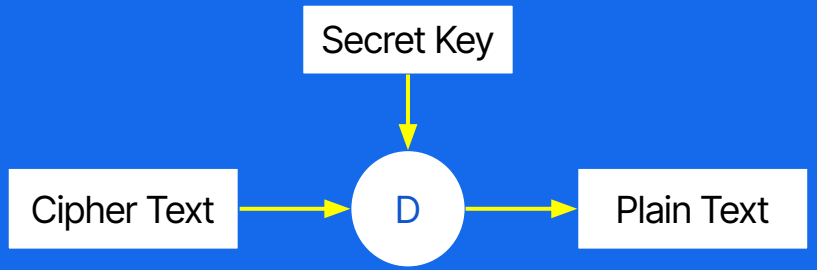


Shannon's Maxim

The enemy knows the system.

Kerckhoffs's Principle

A cryptosystem should be secure, even if everything about the system except the key is public knowledge.



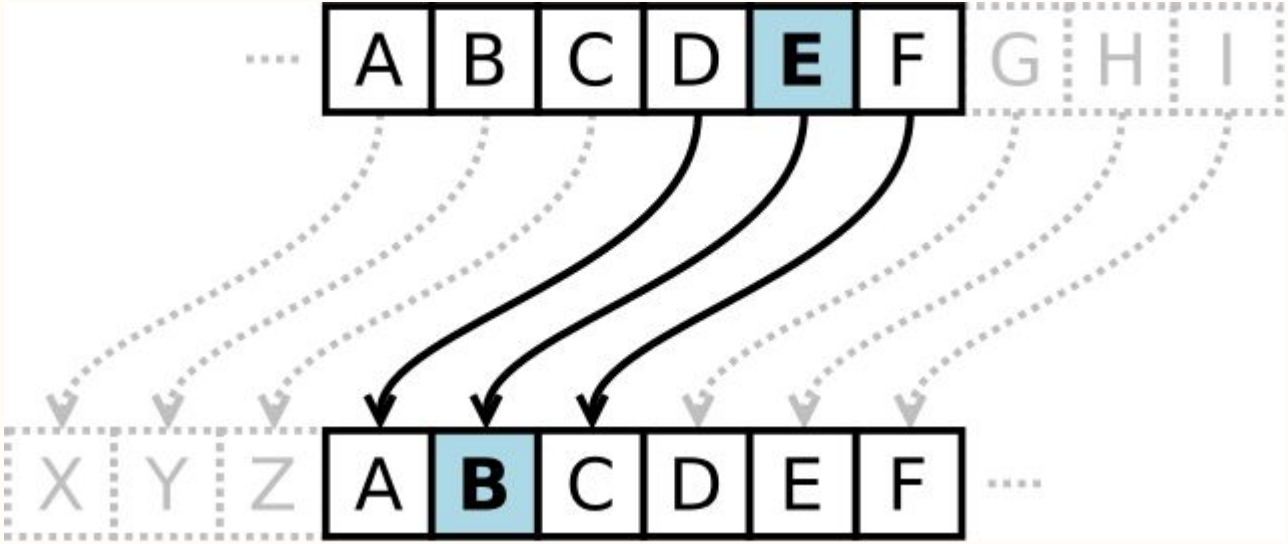
Caesar cipher

- ➔ Developed in ancient Rome
- ➔ Named after Julius Caesar

$$E_n(x) = (x + n) \ mod \ 26$$

$$D_n(x) = (x - n) \ mod \ 26$$

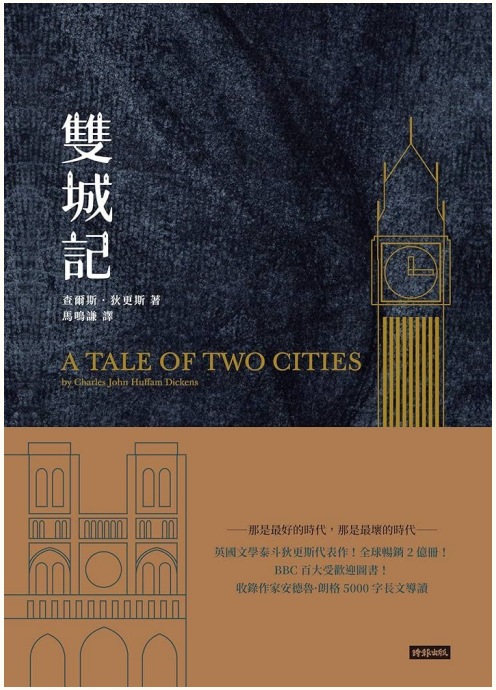
Secret Key



Mixed Alphabet cipher

Example:

It was the best of times, it was the worst of times.
>>>
Er vpq rda xaqr kb reiaq, er vpq rda vkoqr kb reiaq.



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

Secret Key

What is Cryptanalysis?

The process of analyzing information systems in order to understand hidden aspects of the systems. It's used to gain access to the contents of encrypted messages, even if the key is unknown.

Brute Force Attack

Caesar cipher

It can be easily broken even in a ciphertext-only scenario. Since there are only a limited number of possible shifts, an attacker can try decrypting with all possible keys and find out the one which generates the meaningful plaintext.

Total possible keys: 25.

Frequency Analysis

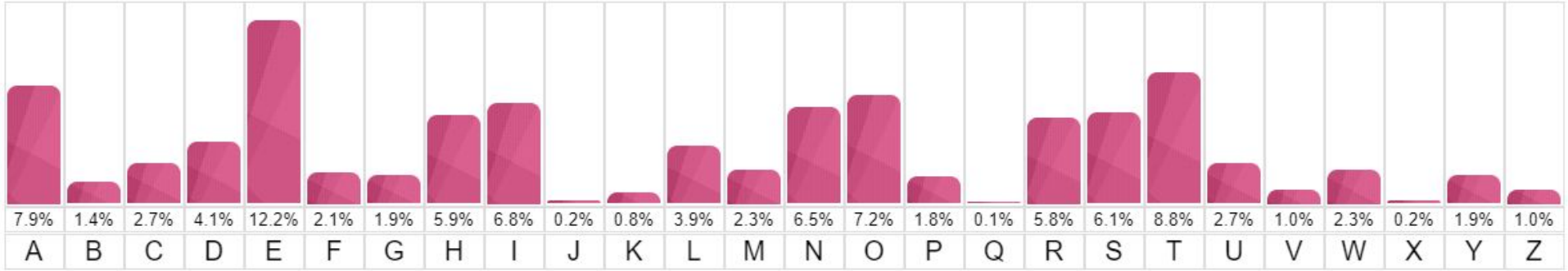
Mixed Alphabet cipher

Q: How many possible keys does it support?

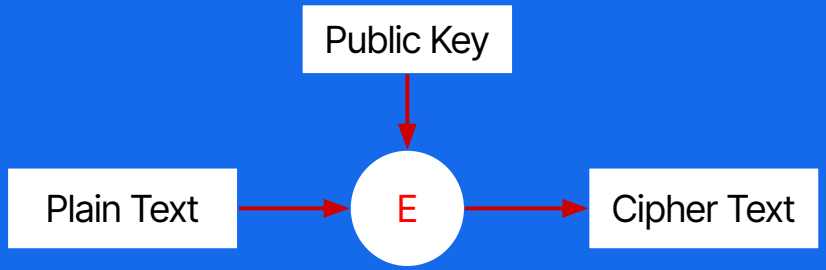
Analyzing the frequency distribution of the ciphertext allows formation of partial words, which can be tentatively filled in, progressively expanding the solution.

Known-plaintext Attack

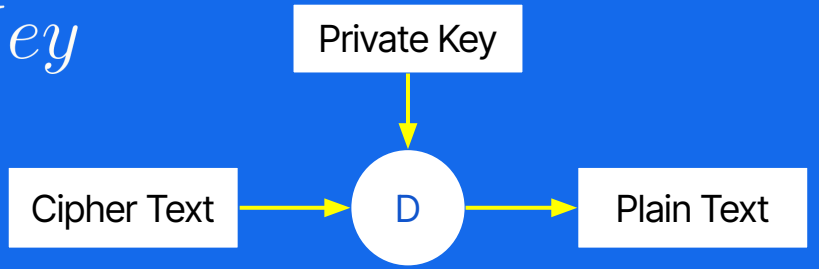
AF is short of water.



Encryption & Decryption



$$Public\ Key\ != \ Private\ Key$$

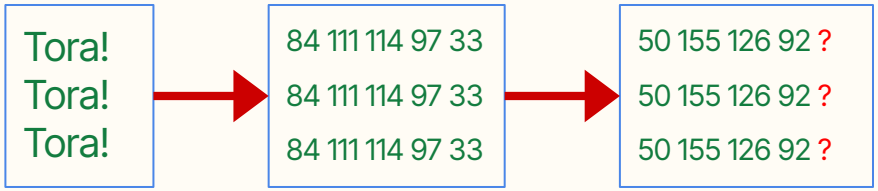


RSA: Example

$$c = p^e \ mod \ n$$
$$p = c^d \ mod \ n$$

Public Key: (n = 187, e = 7)

Private Key: (n = 187, d = 23)



$$84^7 \ mod \ 187 = 50$$
$$111^7 \ mod \ 187 = 155$$

$$50^{23} \ mod \ 187 = 84$$
$$155^{23} \ mod \ 187 = 111$$

Q: What is the last cypher number?

RSA: the Magic Numbers

1) Choose two large prime numbers p and q randomly.
2) Let $n = pq$.
3) Let $\varphi = (p - 1)(q - 1)$.
4) Choose a large number $e \in [2, \varphi - 1]$ that is coprime to φ.
5) Compute $d \in [2, \varphi - 1]$ such that

   $$e \cdot d = 1 \pmod{\varphi}$$

   There is a unique such d. Furthermore, d must be coprime to φ.
6) Announce to the whole word the pair (e, n), which is the public key.
7) Keep d secret, and the private key is (d, n).

RSA: the Truth behind Magic

Definition

Given an integer p > 0, define $\mathbb{Z}_p$ as the set {0, 1, ..., p − 1}.

Fermat's Little Theorem

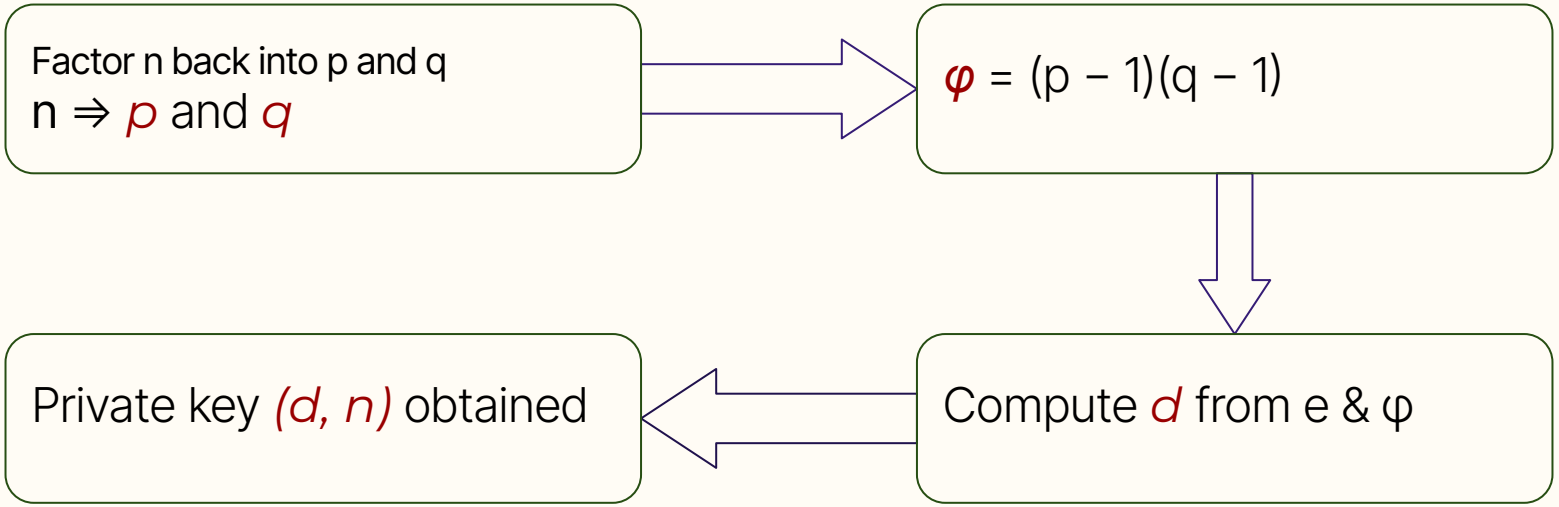
If p is a prime number, for any non-zero a ∈ $\mathbb{Z}_p$, it holds that

$$a^{p-1} = 1 \ mod \ p.$$

Chinese Remainder Theorem

Let p and q be two co-prime integers. If x = a mod p and x = a mod q, then x = a mod pq.

RSA: How to Break?



Assumption

Factoring large integers is computationally impossible.

Questions?

References

1. Battle of Midway (Wikipedia)
2. Purple (Grand Valley State University)
3. Genevieve Grotjan Feinstein (Wikipedia)
4. Marian Rejewski (Wikipedia)
5. Type B Cipher Machine (Wikipedia)
6. Operation Vengeance (The National WWII Museum)
7. Frequency Analysis (101 Computing)
8. RSA Cyrptosystem & Correctness of RSA (Prof Yufei Tao, CUHK)

Available on GitHub