RSA Cryptography

Carolyn Zhang, Tara Zhan, and Ryan Denomey (Team Pascal)

Supervisor: Dr. Liprandi

May 2021

All About RSA Encryption

History of RSA and Public Key Cryptography

The Math Behind RSA Encryption

Everyday Uses For RSA

Breaking RSA With Quantum Computers

A

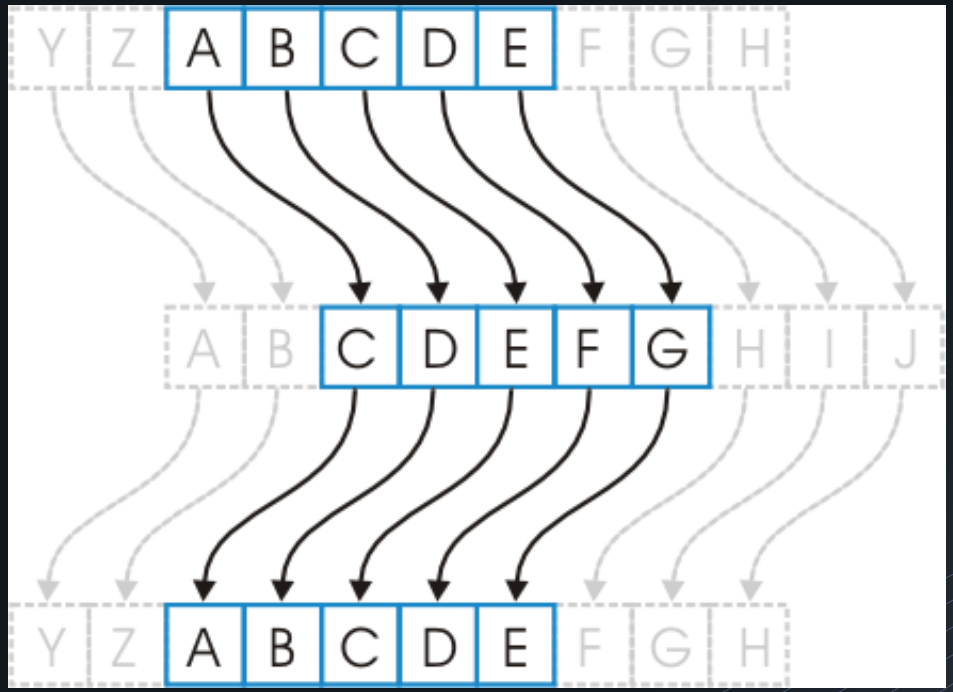
The History of RSA

The History of Cryptography

The first recorded uses of cryptography date back to Ancient Egypt (circa 2000 BC), when scribes encrypted the messages of the kings with hieroglyphs.

Hieroglyphs dated from 1900 BCE

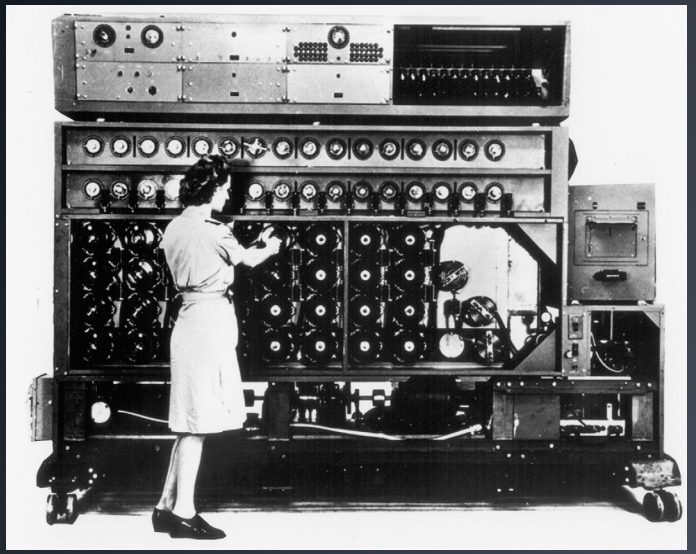
As writing evolved, around 500 BC, Julius Caesar used the Caesar Shift Cipher to encode the messages he sent.



- Letters are shifted forward by three positions to encrypt a ciphertext.
- The reverse operation is done to decrypt.

One of the most recognizable earlier forms of cryptography is the Enigma rotor machine, which was widely used by Nazi Germany during World War II.

An Enigma encryption machine



The Enigma decryption machine

Public-Key Cryptography

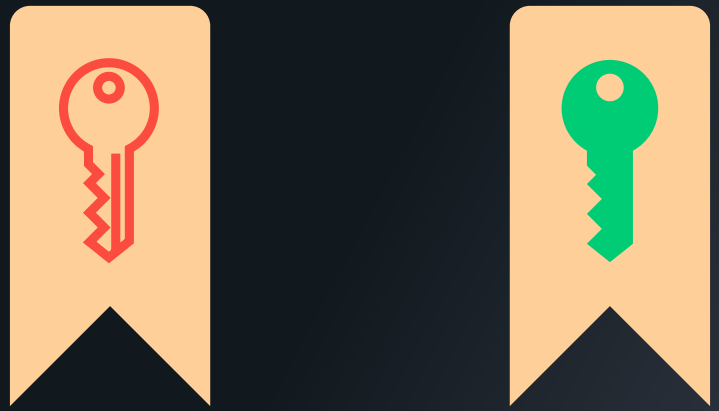
Third-party interceptor

Up until the 20th century, sending messages through encryption faced a major problem— key distribution. In private-key encryption, the same key is used for encrypting and decrypting the message.

Sender

Recipient

In 1977, Whitfield Diffie, an American cryptographer, came up with the concept of asymmetric (public-key) cryptography, a method that would employ two different keys.

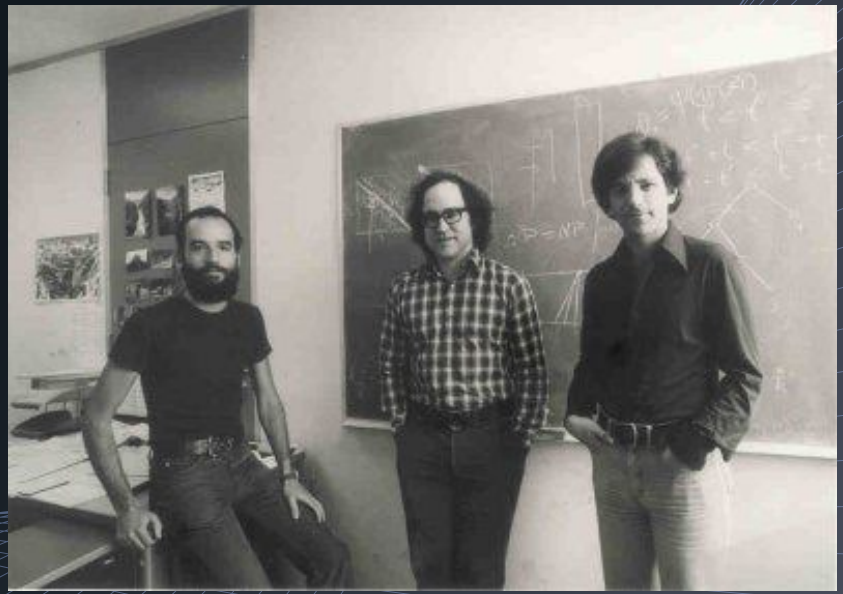


The public key would be used to encrypt the message, whereas the private would be used to decrypt.

The Origins of RSA Cryptography

RSA was developed by Ronald Rivest, Adi Shamir, and Leonard Adleman at the Massachusetts Institute of Technology (MIT) in 1977.

Over the course of one year, they had generated 42 failed attempts at creating a satisfactory one-way function.

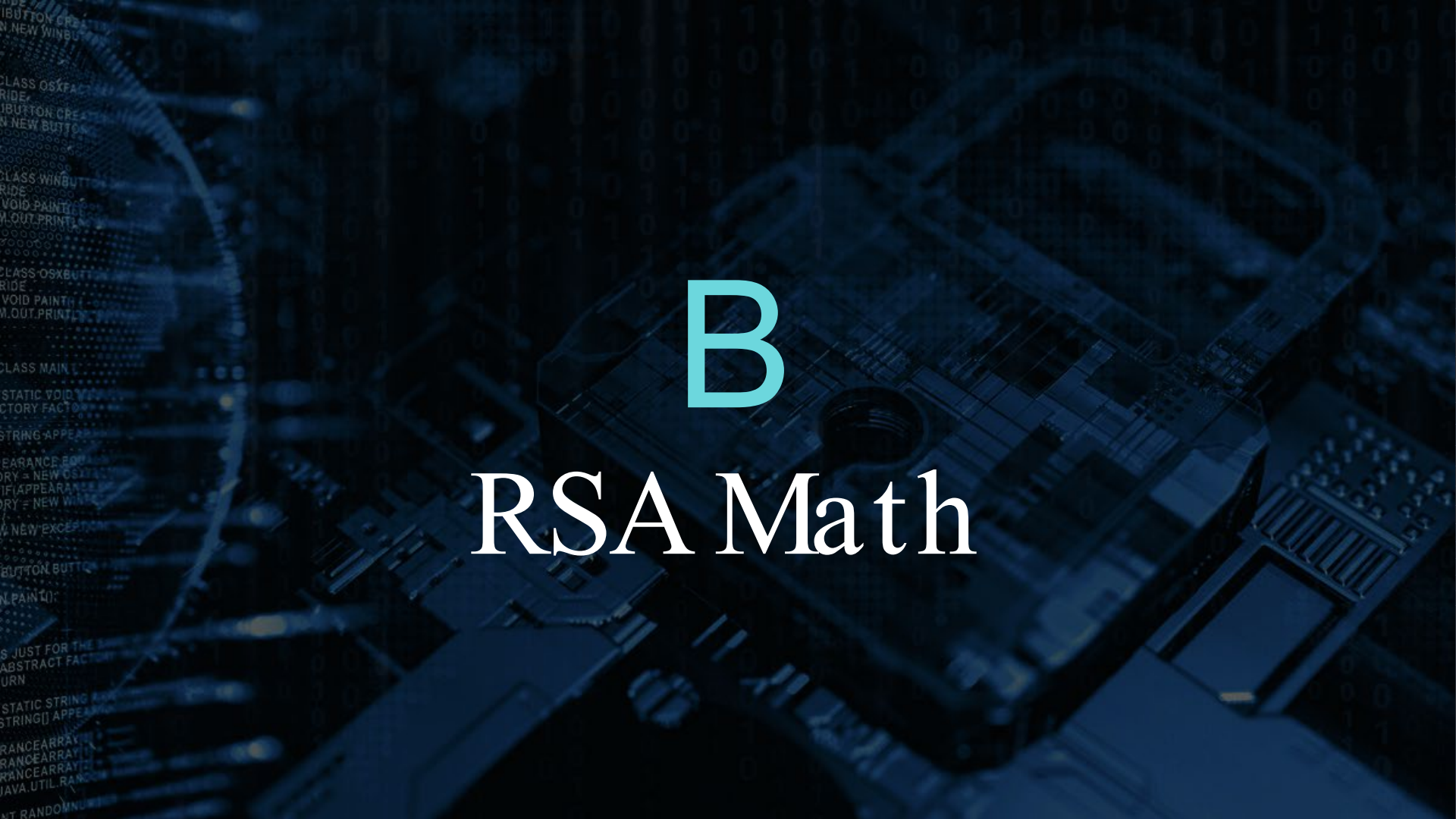


Bob

Alice

Bob's open padlock
(the *public* key)

Bob's lock key
(the *private* key)



B

RSA Math

Overview

1 The receiver's **public key** is generated (**n** and **e**)

2 The receiver's **private key** is generated (**d**)

3 The sender converts their message into **m** and **encrypts** it into the ciphertext (**c**)

4 The receiver **decrypts** the ciphertext to retrieve the message

1.

Public Key

Generating **n** and **e**

$n = pq$ ⟶ *one-way function*

- p and q are very large prime numbers

EASY: multiplying p × q to get n

DIFFICULT: prime factoring n to get p and q

Euler's totient function: φ(k)

- **φ(k)**, k∈ℤ returns the number of integers between 1 and k that are **relatively prime** to k (i.e. gcd is 1)
- E.g. **φ(5) = 4**, since 1, 2, 3, and 4 are each relatively prime to it

Question 1a: What is φ(10) ?

φ(10) = 4

since gcd(1, 10) = gcd(3, 10) = gcd(7, 10) = gcd (9, 10) = 1

Question 1b: What is φ(11) ?

φ(11) = 10

since gcd(1, 11) = gcd(2, 11) = gcd(3, 11) = gcd(4, 11) = gcd(5, 11) = gcd(6, 11) = gcd (7, 11) = gcd(8, 11) = gcd(9, 11) = gcd(10, 11) = 1

Do you notice anything?

Properties of Euler's totient function

- If r is prime, then $\varphi(r) = r-1$

  Prime number: a natural number whose only factors are 1 and itself

- If $n = pq$ and $\gcd(p, q) = 1$, then $\varphi(n) = \varphi(p)\varphi(q)$

- If p and q are prime, then $\varphi(n) = (p-1)(q-1)$

e

$$\gcd(e, \varphi(n)) = 1$$

In practice, **e** is generally chosen to be $2^{16} + 1 = 65537$

n = pq

gcd(e, **φ**(n)) = 1

2.

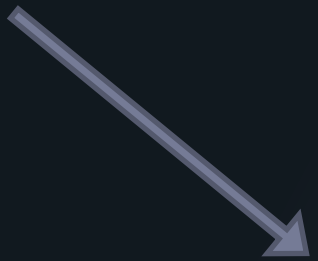
Private Key 

Generating **d**

Private Key: d

d is the *modular multiplicative inverse* of e (mod φ(n)) :

$$de \equiv 1 (\mathrm{mod}\ \varphi(n))$$



MODULAR ARITHMETIC

Modular Arithmetic

Finding the remainder when one number is divided by another

For example,

$36 \equiv 8 \pmod 7$

since both have R 1 when divided by 7

If $x \equiv y \pmod z$, then

- $y \equiv x \pmod z$
- $x = kz + y$, $k \in \mathbb{Z}$
- $x - y \equiv 0 \pmod z$

Question 2a: Determine a value of y that satisfies $34 \equiv y \pmod 7$.

Using the 1st property, we can rewrite the question as

$y \equiv 34 \pmod 7$

$y \equiv 6 \pmod 7$

Using the 2nd property, we can introduce a variable, k, $k \in \mathbb{Z}$

$y = 7k + 6$

Substituting in integer values for k, we obtain

y = ... -8, -1, 6, 13...

Modular Arithmetic

Finding the remainder when one number is divided by another

For example,

$36 \equiv 8 \pmod 7$

since both have R 1
when divided by 7

If $x \equiv y \pmod z$, then

- $y \equiv x \pmod z$
- $x = kz + y$, $k \in \mathbb{Z}$
- $x - y \equiv 0 \pmod z$

Question 2b: Determine a value of z that satisfies $36 \equiv 10 \pmod z$.

Using the 3rd property, we can rewrite this as

$(36 - 10) \equiv 0 \pmod z$

$26 \equiv 0 \pmod z$

This means that z is a factor of 26.

26: {1, 2, 13, 26}

Since z could be any of these values,

$z = 1, 2, 13, 26$

Operations in Modular Arithmetic

Addition

- If $a + b = c$, then $a \pmod N + b \pmod N \equiv c \pmod N$

Multiplication

- If $a \times b = c$, then $a \pmod N \times b \pmod N \equiv c \pmod N$

Example: What is the remainder when $123 + 234 + 32 + 56 + 22 + 12 + 78$ is divided by 3?

$123 + 234 + 32 + 56 + 22 + 12 + 78 \pmod 3 \equiv 0 + 0 + 2 + 2 + 1 + 0 + 0 \pmod 3$

$123 + 234 + 32 + 56 + 22 + 12 + 78 \pmod 3 \equiv 5 \pmod 3$

$123 + 234 + 32 + 56 + 22 + 12 + 78 \pmod 3 \equiv 2 \pmod 3$

Private Key: d

$$de \equiv 1 \pmod{\varphi(n)}$$

$$de = 1 + k\,\varphi(n),\ k \in \mathbb{Z}$$

$$de - k\,\varphi(n) = 1$$

$$\varphi(n) = (p - 1)(q - 1)$$

How can we find d?

- We have the values of **φ(n)** and **e**, which we can substitute into the equation
- More than one value of d could satisfy the equation

Apply the Extended Euclidean algorithm to de - k φ(n) = 1

Public Key

$n = pq$

$\gcd(e, \varphi(n)) = 1$

Private Key

$de \equiv 1 \pmod{\varphi(n)}$

3.

Encryption

Conversion of m and computation of c

Converting plaintext into m

$m < n$

ASCII printable characters

32	space	64	@	96	`
33	!	65	A	97	a
34	"	66	B	98	b
35	#	67	C	99	c
36	$	68	D	100	d
37	%	69	E	101	e
38	&	70	F	102	f
39	'	71	G	103	g
40	(	72	H	104	h
41	)	73	I	105	i
42	*	74	J	106	j
43	+	75	K	107	k
44	,	76	L	108	l
45	-	77	M	109	m
46	.	78	N	110	n
47	/	79	O	111	o
48	0	80	P	112	p
49	1	81	Q	113	q
50	2	82	R	114	r
51	3	83	S	115	s
52	4	84	T	116	t
53	5	85	U	117	u
54	6	86	V	118	v
55	7	87	W	119	w
56	8	88	X	120	x
57	9	89	Y	121	y
58	:	90	Z	122	z
59	;	91	[	123	{
60	<	92	\	124	|
61	=	93	]	125	}
62	>	94	^	126	~
63	?	95	_		

Example:
Convert the message *H3LLO!*

H = 72

3 = 72

L = 76

L = 76

O = 79

! = 33

Ciphertext: c

$$c \equiv m^e \pmod{n}$$

Modular logarithms → difficult!

4.

Decryption

Retrieval of m

Decryption formula

$$c^d \equiv m \pmod{n}$$

or

$$m \equiv c^d \pmod{n}$$

Proof of $c^d = m \pmod n$

Equations

Ciphertext formula:

- $c \equiv m^e \pmod n$

Private key formula:

- $de = 1 + k\,\varphi(n)$

Euler's theorem:

- $m^{\varphi(n)} \equiv 1 \pmod n$

$$
\begin{aligned}
c &\equiv m^e \pmod n \\
c^d &\equiv (m^e)^d \pmod n \\
c^d &\equiv m^{de} \pmod n \\
c^d &\equiv m^{1 + k\,\varphi(n)} \pmod n \\
c^d &\equiv m^1 \times m^{k\,\varphi(n)} \pmod n \\
c^d &\equiv m \times (m^{\varphi(n)})^k \pmod n \\
c^d &\equiv m \times (1)^k \pmod n \\
c^d &\equiv m \pmod n
\end{aligned}
$$

Example: RSA Simulation

Question 3a: Given that p = 11, q = 17, and e = 3, determine the receiver's public and private keys.

Public key – n and e

$n = pq$

$n = (11)(17)$

$n = 187$

$e = 3$

Private key – d

$de \equiv 1 \pmod{\varphi(n)}$

$3d \equiv 1 \pmod{(p-1)(q-1)}$

$3d \equiv 1 \pmod{(11-1)(17-1)}$

$3d \equiv 1 \pmod{160}$

$3d = 1 + 160k$

$3d - 160k = 1$

$3(107) - 160(2) = 1$

$d = 107$

Example: RSA Simulation

Question 3b: Encrypt the letter *M* into the ciphertext, c, using the ASCII conversion table to obtain m.

ASCII printable characters

32	space	64	@	96	`
33	!	65	A	97	a
34	"	66	B	98	b
35	#	67	C	99	c
36	$	68	D	100	d
37	%	69	E	101	e
38	&	70	F	102	f
39	'	71	G	103	g
40	(	72	H	104	h
41	)	73	I	105	i
42	*	74	J	106	j
43	+	75	K	107	k
44	,	76	L	108	l
45	-	77	M	109	m
46	.	78	N	110	n

47	/	79	O	111	o
48	0	80	P	112	p
49	1	81	Q	113	q
50	2	82	R	114	r
51	3	83	S	115	s
52	4	84	T	116	t
53	5	85	U	117	u
54	6	86	V	118	v
55	7	87	W	119	w
56	8	88	X	120	x
57	9	89	Y	121	y
58	:	90	Z	122	z
59	;	91	[	123	{
60	<	92	\	124	|
61	=	93	]	125	}
62	>	94	^	126	~
63	?	95	_		

Recall from Question 3a:
$n = 187$, $e = 3$

Message - m

$m = 77$

Ciphertext – c

$c \equiv m^e \pmod{n}$

$c \equiv 77^3 \pmod{187}$

$c \equiv 456533 \pmod{187}$

$c = 66$

Example: RSA Simulation

Question 3c: Use the decryption formula to retrieve the sender's message, m.

Recall from Questions 3a and 3b: $c = 66$, $d = 107$, $n = 187$

$m \equiv c^d \pmod{n}$

$m \equiv 66^{107} \pmod{187}$

How can we calculate $66^{107} \pmod{187}$?

Fast Modular Exponentiation

How can we calculate $66^{107} \pmod{187}$?

1. Convert the exponent, 107, to base two

$107_{ten} = 1101011_{two}$

Start at 66^0:

2. Square the previous number, then take the mod 187.

3. Look at the base two number: 1101011

Starting from the leftmost digit,

If the digit is a 1, multiply by the base, 66, then take the mod 187. If the digit is a 0, do nothing.

Repeat for each digit in the base two number

Base 2 Digit	Step	Calculation	(mod 187)
1	Square	$(66^0)^2 = 66^0$	$66^0 \pmod{187} = 1$
	Multiply	$66^0 \times 66^1 = 66^1$	$1 \times 66 \pmod{187} \equiv 66 \pmod{187} = 66$
1	Square	$(66^1)^2 = 66^2$	$66^2 \pmod{187} \equiv 4356 \pmod{187} = 55$
	Multiply	$66^2 \times 66^1 = 66^3$	$55 \times 66 \pmod{187} \equiv 3630 \pmod{187} = 77$
0	Square	$(66^3)^2 = 66^6$	$77^2 \pmod{187} \equiv 5929 \pmod{187} = 132$
1	Square	$(66^6)^2 = 66^{12}$	$132^2 \pmod{187} \equiv 17424 \pmod{187} = 33$
	Multiply	$66^{12} \times 66^1 = 66^{13}$	$33 \times 66 \pmod{187} \equiv 2178 \pmod{187} = 121$
0	Square	$(66^{13})^2 = 66^{26}$	$121^2 \pmod{187} \equiv 14641 \pmod{187} = 55$
1	Square	$(66^{26})^2 = 66^{52}$	$55^2 \pmod{187} \equiv 3025 \pmod{187} = 33$
	Multiply	$66^{52} \times 66^1 = 66^{53}$	$33 \times 66 \pmod{187} \equiv 2178 \pmod{187} = 121$
1	Square	$(66^{53})^2 = 66^{106}$	$121^2 \pmod{187} \equiv 14641 \pmod{187} = 55$
	Multiply	$66^{106} \times 66^1 = 66^{107}$	$55 \times 66 \pmod{187} \equiv 3630 \pmod{187} = 77$

Example: RSA Simulation

Question 3c: Use the decryption formula to retrieve the sender's message, m.

Recall from Questions 3a and 3b: c = 66, d = 107, n = 187

$m \equiv c^d \pmod{n}$

$m \equiv 66^{107} \pmod{187}$

$m = 77$

The sender's message is "M"!

ASCII printable characters

32	space	64	@	96	`
33	!	65	A	97	a
34	"	66	B	98	b
35	#	67	C	99	c
36	$	68	D	100	d
37	%	69	E	101	e
38	&	70	F	102	f
39	'	71	G	103	g
40	(	72	H	104	h
41	)	73	I	105	i
42	*	74	J	106	j
43	+	75	K	107	k
44	,	76	L	108	l
45	-	77	M	109	m
46	.	78	N	110	n

C

Applications of RSA

Time Stamping

- This can be used to certify that something was delivered at a certain time.
- RSA encryption helps this stay secure.

Electronic Money

- Money can be transferred through the internet.
- RSA helps secure this process.

Secure Network Communications

- Secure Socket Layer is a form of public key encryption.
- It was created using RSA's basic functions.
- It is used for securing data and authenticating connection to internet based communication.

Anonymous Remailers

- Removes your identity when you send an email.
- A remailer keeps your identity.
- Encrypt the message using the final remailer's public key.

How to Gain More Knowledge

- Ethical hacking contests with RSA encryption problems
- PicoCTF

- Many problems that I was able to crack using tools like prime factorization tools, ascii converters, base 16 and base 64 converters.

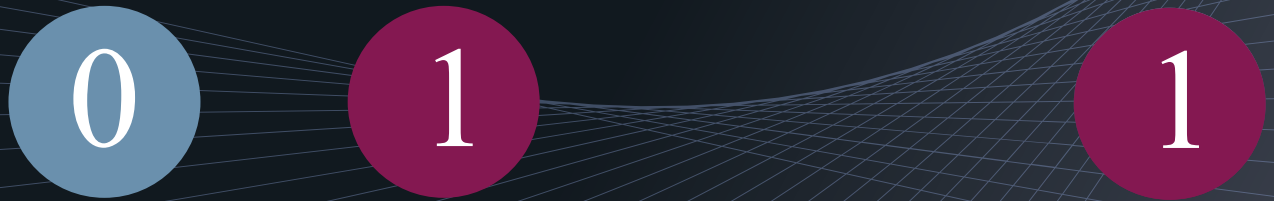
Breaking RSA

What quantum computing means for cryptography

What is quantum computing?

An ordinary computer uses bits to store data in the forms of 0s and 1s.

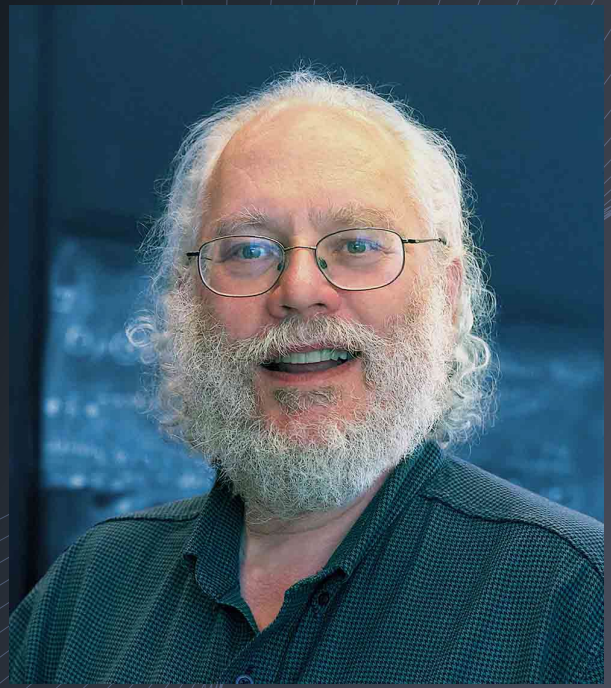
Quantum computers use qubits, which can be set to 0 and 1 at the same time, or even a combination of the two.



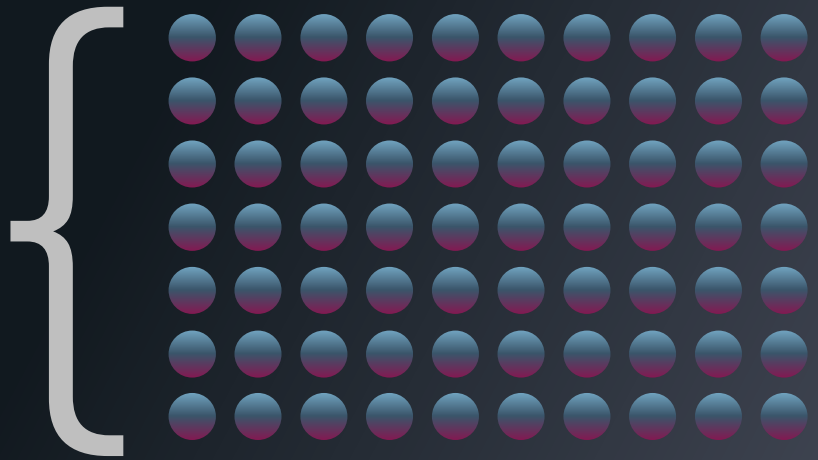
Shor’s algorithm

- In 1994, a mathematician named Peter Shor developed an algorithm for quantum computers that could break encryption methods like RSA.

- Shor’s algorithm breaks down the prime factorization of any integer into 3 parts.



The current best quantum computers in the world have around 70 stable qubits.



To crack standard 2048-bit RSA, a quantum system would require 20,000,000 working qubits and 8 hours of computing time.

way too many

Solutions

Quantum-resistant algorithms

- Many quantum-resistant algorithms that can
- replace RSA exist. However, they have not been proven fully quantum-proof.

Quantum key distribution

- In the world of quantum physics, subatomic particles
- behave in such a way that simply observing them will change their structure.

Third-party interceptor

Sender

. . . ?

Recipient

Thank you!