An Introduction to Mathematical Cryptography

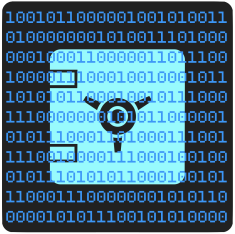
James Guo

January 18th, 2024

Contents:

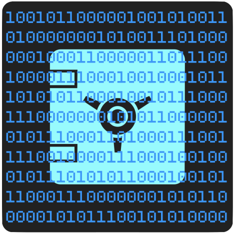
What is Cryptography

- Cryptography is a subject under mathematics.
- Cryptography involves encrypting and decrypting codes.
- The goal of cryptography is to encode your message with someone so that others cannot understand.



What is Cryptography

- Cryptography is a subject under mathematics.
- Cryptography involves encrypting and decrypting codes.
- The goal of cryptography is to encode your message with someone so that others cannot understand.



Types of Cryptography

- Regular approaches have both Encryption and Decryption methods keep as secret.
- Public RSA releases the Encryption method to the public and keeps the Decryption method as secret.

A Story about Mary Queen of Scots

Figure of Queen Mary

- Queen Mary was a queen of Scotland, and she was put on a prosecution on whether she committed treason.
- Luckily, she has all the evidences about her treason encrypted by a cipher. The security of this cipher decides her fate.

A Story about Mary Queen of Scots

Figure of Queen Mary

- Queen Mary was a queen of Scotland, and she was put on a prosecution on whether she committed treason.
- Luckily, she has all the evidences about her treason encrypted by a cipher. The security of this cipher decides her fate.
- Queen Mary's story ended with the result that her ciphers were cracked, announcing her death trail later.

Discussion

Should cryptography (possibly part of privacy) be encouraged, or be better monitored to prevent it being used for illegal things?

A Story about Mary Queen of Scots

Figure of Queen Mary

- Queen Mary was a queen of Scotland, and she was put on a prosecution on whether she committed treason.
- Luckily, she has all the evidences about her treason encrypted by a cipher. The security of this cipher decides her fate.
- Queen Mary's story ended with the result that her ciphers were cracked, announcing her death trail later.

Other Stories about Cryptography

More examples from *The Code Book - The Science of Secrecy from Ancient Egypt to Quantum Cryptography* (1999) by Simon Singh.

Euler's Theorem

You might have heard about Fermat's Little Theorem, but now shall we introduce a stronger theorem, known as Euler's Theorem.

Euler's Theorem

Let $m \in \mathbb{Z}^+$ and $a \in \mathbb{Z}$. If $\gcd(a, m) = 1$, then $a^{\phi(m)} \equiv 1 \mod m$, where $\phi(m)$ is defined by the number of elements in $\{n \in \mathbb{Z} : 0 \leq n \leq m - 1, \gcd(n, m) = 1\}$.

If you are interested in the proof of Euler's Theorem, you may find it on the provided handout.

Euler's ϕ Function

Being introduced to Euler's ϕ function, it is important to know its calculations, as follows:

Prepositions on Euler's ϕ Function

Let p be a prime, n as an integer, then

$$\phi(p^n) = p^n - p^{n-1}.$$

Let m and n be integers such that $\gcd(m, n) = 1$, then

$$\phi(mn) = \phi(m)\phi(n).$$

Similarly, if you are interested in the proof of the calculation, you may find a sketch of it on the provided handout.

Group Theory

You might have found the above proofs lengthy. With the developments of Modern Algebra (or Abstract Algebra), one can prove it in a more canonical approach.

Even without sufficient context, some smart readers might have noticed that the multiplications forms a "cycle", noted as a **Cyclic group** in **Group theory**.

Group Theory

Now, here we have a brief introduction to **Groups Structure**, which is a useful Algebraic Structure in mathematics.

Group Theory

Now, here we have a brief introduction to **Groups Structure**, which is a useful Algebraic Structure in mathematics.

Group Theory (Brief Introduction)

One could consider a set G and a binary operator $\bullet_G : G \to G$ a **group** if it satisfies the following:

1. $\bullet_G$ is associative:
   $(\forall g, h, k \in G) : \ (g \bullet_G h) \bullet_G k = g \bullet_G (h \bullet_G k);$
2. There exists an identity element e_G:
   $(\exists e_G \in G)(\forall g \in G) : \ g \bullet_G e_G = g = e_G \bullet_G g;$
3. Every element has an inverse with respect to $\bullet_G$:
   $(\forall g \in G)(\exists h \in G) : \ g \bullet_G h = e_G = h \bullet_G g.$

Furthermore, **Group Theory** can be understood by **Category Theory**, which is more general.

Group Theory

Without additional contexts, we may consider G consists powers of a modulo m with multiplications as operator, denoted $(G, \cdot)$, as follows:

$$\begin{tikzcd} a \arrow[r, "\cdot a"] & a^2 \arrow[r, "\cdot a"] & \cdots \arrow[r, "\cdot a"] & a^{\phi(m)-1} \arrow[r, "\cdot a"] & a^{\phi(m)} \equiv 1 \arrow[llll, bend left, "\cdot a"] \end{tikzcd}$$

Cyclic Group

Notation-wise, this can be considered as a **Cyclic group** generated by a single element a. There are more discussions on order and index of groups.

Group Theory

Without additional contexts, we may consider G consists powers of a modulo m with multiplications as operator, denoted $(G, \cdot)$, as follows:

$$
\begin{tikzcd}
a \arrow[r, "\cdot a"] & a^2 \arrow[r, "\cdot a"] & \cdots \arrow[r, "\cdot a"] & a^{\phi(m)-1} \arrow[r, "\cdot a"] & a^{\phi(m)} \equiv 1 \arrow[llll, bend left, "\cdot a"]
\end{tikzcd}
$$

Cyclic Group

Notation-wise, this can be considered as a **Cyclic group** generated by a single element a. There are more discussions on order and index of groups.

This is a very brief example of **Group Theory** from Abstract Algebra. If you found this interesting, consider taking some college level courses on such topic.

Public RSA

With sufficient mathematical background, we may come back to cryptography, what we want the most is to find some algorithms for public RSA.

Public RSA

We want to find a way to encrypt to the public while having a secret way to encrypt it.

Public RSA

With sufficient mathematical background, we may come back to cryptography, what we want the most is to find some algorithms for public RSA.

Public RSA

We want to find a way to encrypt to the public while having a secret way to encrypt it.

This must sound counter-intuitive for many of you, as we have learned about inverse functions. For many elementary functions, there exists an inverse function that 'undo' the operation.

Public RSA

Public RSA

We want to find a way to encrypt to the public while having a secret way to encrypt it.

Therefore, mathematicians jumped out of the elementary function, and had their attention to more complicated operations.

Public RSA

Public RSA

We want to find a way to encrypt to the public while having a secret way to encrypt it.

Therefore, mathematicians jumped out of the elementary function, and had their attention to more complicated operations.

Eventually, they had their attention towards modular arithmetic, where the 'undo' process is as hard for the decrypts even if people know everything about the operation.

Public RSA Algorithm

Utilizing Euler's Theorem, we can develop the following algorithms with public keys (n, r) such that n is the product of two prime numbers p_1 and p_2, while $\gcd(\phi(n), r) = 1$. The original message could be an integer M.

Process of Public RSA

$$\begin{tikzcd}
\textbf{Encoder} & M \arrow[r] & M^r \bmod n \arrow[r] & E \arrow[ddr] & \\
\textbf{Public} & (n, r) \arrow[ur] \arrow[dr] & & & \\
\textbf{Decoder} & n = p_1 \times p_2 \arrow[u] & r^{-1} \bmod \phi(n) \arrow[r] & s \arrow[r] & E^s \bmod n \to M \\
& (p_1, p_2) \arrow[u] \arrow[r] & \phi(n) = (p_1 - 1)(p_2 - 1) \arrow[u] & &
\end{tikzcd}$$

Public RSA Algorithm

Process of Public RSA

$$
\begin{tikzcd}
\textbf{Encoder} & M \arrow[r] & M^r \bmod n \arrow[rr] & & E \arrow[dd] & \\
\textbf{Public} & (n, r) \arrow[ur] \arrow[dr] & & & & \\
\textbf{Decoder} & n = p_1 \times p_2 \arrow[u] & r^{-1} \bmod \phi(n) \arrow[r] & s \arrow[r] & E^s \bmod n \arrow[r] & M \\
& (p_1, p_2) \arrow[u] \arrow[r] & \phi(n) = (p_1 - 1)(p_2 - 1) \arrow[u] & & &
\end{tikzcd}
$$

You might now be wondering why this is secure. The key is on factoring a composite number. Although it does not sound that hard, factoring is quite hard when it comes to large prime numbers.

Example of Public RSA

For simplicity, here is an example with small primes demonstration the encrypting and decrypting 30 using public key $(221, 101)$:

$$
\begin{tikzcd}
 & \text{Message: } 30 \arrow[r] & 30^{101} \bmod 221 \equiv 166 \arrow[r] & 166 \arrow[dddl, bend left] \\
 & \text{Key: } (221, 101) \arrow[ur] & & \\
\text{Primes: } (13, 17) \arrow[r] \arrow[dr] & 13 \times 17 = 221 \arrow[u] & 101^{-1} \bmod 192 \equiv 173 \arrow[d] & \\
 & \phi(221) = 12 \times 16 = 192 \arrow[ur] & 166^{173} \bmod 221 = \boxed{30} &
\end{tikzcd}
$$

Note: You should consider using Wolfram Alpha, or other equivalent tools, for the scope of calculation.

Security for Public RSA

In reality, there is not yet a sufficient algorithm to factor large numbers into primes.

Application of Public RSA

Governments, banking services, and many services use this Public RSA systems.

Security for Public RSA

In reality, there is not yet a sufficient algorithm to factor large numbers into primes.

Application of Public RSA

Governments, banking services, and many services use this Public RSA systems.

People might ask: Are there infinitely many prime numbers? There is an exquisite proof by contradiction.

Proof.

Assume that there exists a finite number of primes, denoted $\{2, 3, 5, \cdots, p_n\}$. We know that $2 \times 3 \times 5 \times \cdots \times p_n + 1$ is not divisible by any of the prime numbers, which is a contradiction. Hence, there does not exist the largest prime, meaning there are infinitely many of them. $\square$

Future for Public RSA

When the primes are hundreds or thousands digits long, the time to crack this cipher is too long to be considered.

Future about Public RSA

However, with potentials of quantum computing and newly developed algorithms, this version of Public RSA is not necessarily safe.

It is important for people to develop new "one-way" functions to secure the message encryption.

Discussion

The advancements in solving these problems are pushing mathematics and other areas of science to newer generations, how shall we evaluate these?

Foundations from Computer Science

As our algorithms are encrypting/decrypting numbers rather than words, so we need to create a one-to-one map (so called *injection*) from each letter/character to a number.

`ASCII` Table

Specifically for Latin letters, one prevailing standard now is the American Standard Code for Information Interchange (or `ASCII`), so each character can be mapped to a unique number between 0 and 127 (inclusive).

Note that if you are familiar with computer science, this really relates to the `char` type in many languages like `Java` or `C`, or the `chr()` and `ord()` functions in `Python`.

Foundations from Computer Science

For simplicity of this activity, the `ASCII` Table is provided as follows:

Decimal - Binary - Octal - Hex – ASCII Conversion Chart

Decimal	Binary	Octal	Hex	ASCII	Decimal	Binary	Octal	Hex	ASCII	Decimal	Binary	Octal	Hex	ASCII	Decimal	Binary	Octal	Hex	ASCII
0	00000000	000	00	NUL	32	00100000	040	20	SP	64	01000000	100	40	@	96	01100000	140	60	`
1	00000001	001	01	SOH	33	00100001	041	21	!	65	01000001	101	41	A	97	01100001	141	61	a
2	00000010	002	02	STX	34	00100010	042	22	"	66	01000010	102	42	B	98	01100010	142	62	b
3	00000011	003	03	ETX	35	00100011	043	23	#	67	01000011	103	43	C	99	01100011	143	63	c
4	00000100	004	04	EOT	36	00100100	044	24	$	68	01000100	104	44	D	100	01100100	144	64	d
5	00000101	005	05	ENQ	37	00100101	045	25	%	69	01000101	105	45	E	101	01100101	145	65	e
6	00000110	006	06	ACK	38	00100110	046	26	&	70	01000110	106	46	F	102	01100110	146	66	f
7	00000111	007	07	BEL	39	00100111	047	27	'	71	01000111	107	47	G	103	01100111	147	67	g
8	00001000	010	08	BS	40	00101000	050	28	(	72	01001000	110	48	H	104	01101000	150	68	h
9	00001001	011	09	HT	41	00101001	051	29	)	73	01001001	111	49	I	105	01101001	151	69	i
10	00001010	012	0A	LF	42	00101010	052	2A	*	74	01001010	112	4A	J	106	01101010	152	6A	j
11	00001011	013	0B	VT	43	00101011	053	2B	+	75	01001011	113	4B	K	107	01101011	153	6B	k
12	00001100	014	0C	FF	44	00101100	054	2C	,	76	01001100	114	4C	L	108	01101100	154	6C	l
13	00001101	015	0D	CR	45	00101101	055	2D	-	77	01001101	115	4D	M	109	01101101	155	6D	m
14	00001110	016	0E	SO	46	00101110	056	2E	.	78	01001110	116	4E	N	110	01101110	156	6E	n
15	00001111	017	0F	SI	47	00101111	057	2F	/	79	01001111	117	4F	O	111	01101111	157	6F	o
16	00010000	020	10	DLE	48	00110000	060	30	0	80	01010000	120	50	P	112	01110000	160	70	p
17	00010001	021	11	DC1	49	00110001	061	31	1	81	01010001	121	51	Q	113	01110001	161	71	q
18	00010010	022	12	DC2	50	00110010	062	32	2	82	01010010	122	52	R	114	01110010	162	72	r
19	00010011	023	13	DC3	51	00110011	063	33	3	83	01010011	123	53	S	115	01110011	163	73	s
20	00010100	024	14	DC4	52	00110100	064	34	4	84	01010100	124	54	T	116	01110100	164	74	t
21	00010101	025	15	NAK	53	00110101	065	35	5	85	01010101	125	55	U	117	01110101	165	75	u
22	00010110	026	16	SYN	54	00110110	066	36	6	86	01010110	126	56	V	118	01110110	166	76	v
23	00010111	027	17	ETB	55	00110111	067	37	7	87	01010111	127	57	W	119	01110111	167	77	w
24	00011000	030	18	CAN	56	00111000	070	38	8	88	01011000	130	58	X	120	01111000	170	78	x
25	00011001	031	19	EM	57	00111001	071	39	9	89	01011001	131	59	Y	121	01111001	171	79	y
26	00011010	032	1A	SUB	58	00111010	072	3A	:	90	01011010	132	5A	Z	122	01111010	172	7A	z
27	00011011	033	1B	ESC	59	00111011	073	3B	;	91	01011011	133	5B	[	123	01111011	173	7B	{
28	00011100	034	1C	FS	60	00111100	074	3C	<	92	01011100	134	5C	\	124	01111100	174	7C	|
29	00011101	035	1D	GS	61	00111101	075	3D	=	93	01011101	135	5D	]	125	01111101	175	7D	}
30	00011110	036	1E	RS	62	00111110	076	3E	>	94	01011110	136	5E	^	126	01111110	176	7E	~
31	00011111	037	1F	US	63	00111111	077	3F	?	95	01011111	137	5F	_	127	01111111	177	7F	DEL

Example Algorithm

Here, I choose the public key as $(n, r) = (239812014798221, 103)$. If someone would encrypt `Math!` (where `EOF` implies the end of message), that is encrypted with the following procedure:

$$
\begin{tikzcd}
\texttt{M} \arrow[d] & \texttt{a} \arrow[d] & \texttt{t} \arrow[d] & \texttt{h} \arrow[d] & \texttt{!} \arrow[d] & \texttt{EOF} \arrow[d] \\
77 \arrow[dr] & 97 \arrow[d] & 116 \arrow[dl] & 104 \arrow[dr] & 33 \arrow[d] & 0 \arrow[dl] \\
 & 77097116 \arrow[d] & & & 104033000 \arrow[d] & \\
 & 125110864846083 & & & 10361242333637 &
\end{tikzcd}
$$

I get the message of `(125110864846083,10361242333637)`, and cracking it without the reverse algorithm would be very hard.

Example Algorithm

However, I know how to decrypt it, since I know that $n = 15485863 \times 15485867$ which are two primes, then $\phi(239812014798221) = (15485863 - 1)(15485867 - 1) = 239811983826492$.
Therefore, by $s = 103^{-1} \pmod{239811983826492} \equiv 135039757882879$, I decrypt as follows:

$$\begin{tikzcd}
 & 125110864846083 \arrow[d] & & & 10361242333637 \arrow[d] & \\
 & 77097116 \arrow[dl] \arrow[d] \arrow[dr] & & & 104033000 \arrow[dl] \arrow[d] \arrow[dr] & \\
77 \arrow[d] & 97 \arrow[d] & 116 \arrow[d] & 104 \arrow[d] & 33 \arrow[d] & 0 \arrow[d] \\
\mathtt{M} & \mathtt{a} & \mathtt{t} & \mathtt{h} & \mathtt{!} & \mathtt{EOF}
\end{tikzcd}$$

Your Time to Try

Now, it is your time to try. Utilize the (n, r) pair as above, encode a message (*make sure the message information is appropriate*) in groups, and share the message to other groups so they can attempt cracking it. In case that this did not get through, here are some encrypted messages, try cracking them out:

1. (108574191301791, 67529133963369, 8975687572719, 56565069352803);
2. (57443192555693, 57250895107371, 103055985363721, 23330079327702, 66149892198847, 27482940557182).

Exercises

1. Prove **Fermat's Little Theorem** by **Euler's Theorem**.
   Remark: Fermat's Little Theorem is that:

   if p is a prime and $a \in \mathbb{Z}$, then $a^p \equiv a \mod p$.

2. Prove the **Prepositions on Euler's ϕ Function** using the sketch of proof.

3. A public key is $(239812014798221, 103)$, in which n can be factored as 15485863 and 15485867 that are two prime numbers. Given an encrypted message is 216642813890413, find the original message.

   Remark: You should consider using Wolfram Alpha, or other equivalent tools, for the scope of calculation.

4. Prove that there exist infinitely many primes congruent to 5 modulo 6 based off the proof that there are infinitely many primes.