Cryptography

Chase Wiederstein

2022-10-11

Caesar's Cipher

Cryptography has been around for centuries and is simply a form of communication. The most simple definition of cryptography is the art of creating and interpreting secret messages. To create a secret message is called "encrypting" and to interpret a secret message is called "decrypting."

One of the oldest and most famous methods of cryptography is known as the Caesar's Cipher used in the first century B.C. by Julius Caesar[1]. The Caesar's Cipher is quite simple and is known as a substitution cipher. It is just a shifting of the alphabet. First, assign the numbers 0-25 to the alphabet respectively. Then, the encrypter will choose a shift. Suppose the shift is $n = 2$. Each letter in the alphabet will shift 2 units to the right. A will become 2, B will become 3, C will become 4, and so one. Using modular arithmetic, this can be explained using $E_n(x) = x + n(mod 26)$ where x is the numerical value of the letter and n is the shift value.

After encrypting the message and sending it, decrypting it is just as simple. All the receiver needs is the key to unlocking the message, the shifting value, n. To decrpyt, you simply use the function $D_n(x) = x - n(mod 26)$.

Suppose I want to encrpyt the word "CRYPTOGRAPHY" to send to a fellow classmate using a shift of $n = 5$. First, I plug the numerical number value of each individual character in the string "CRYPTOGRAPHY" into the encrypting equation, $E_n(x) = n + x(mod 26)$.

Table 1: Caesar's Cipher 5 Unit Shift

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Alphabet	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
Caesar	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U

Now, the encrypted message will read the character string of "HWDUYTLWFUMD." To decrypt, the fellow classmate will use the key of $n = 6$ along with the decrypting function $D_n(x) = x - n(mod 26)$ to reverse the shift and read "CRYPTOGRAPHY." However, if the message is intercepted, cracking the encrypted message would take no time at all even without the key. There are only 26 possible combinations of what the shift could be. Over time, this process of creating trickier encryption methods has become much more complex, yet the Caesar Cipher is still a foundational model of how cryptography works.

RSA Cryptography

Since were no longer in Roman times, cryptography has become more important as we communicate globally with the internet. The sharing of credit card numbers, social security, names, etc. online is an everyday occurrence and security for our information is a must. RSA cryptography is one solution protecting us from those who wish to steal our information.

. . . . . Insert history, the names and shit. . . .

RSA uses two keys: a "public key" used for encryption, and a "private key" used for decryption.

RSA Algorithm

The RSA algorithm can be broken up into 3 sections: key generation, encryption, and decryption.

Key Generation Algorithm

Step 1: Find two large primes, p_0 and p_1, such that their product, n, is of the required bit length. These lengths will usually be of the standard 1024, 2048,and 3027 bits. (CITE-pg 22 fips 186-3)

Step 2: Calculate $n = p_0 p_1$ and use Euler's ϕ-Function to calculate $\phi(n) = (p_0 - 1)(p_1 - 1)$.

Step 3: Choose some integer e such that $1 < e < \phi$ and a and ϕ are relatively prime. i.e. $(e, \phi) = 1$.

Step 4: Calculate d, the multiplicative inverse of e. i.e. $d \equiv e^{-1}(mod\phi)$

Step 5: Done! The "public key" is now (n, e) and the "private key" is (n, d).

Finding Large Primes

Calculating large primes for p_0 and p_1 is one of the easier parts of the Key Generation Algorithm with the help of Fermat's Little Theorem and the Primality Test.

Fermat's Little Theorem If p is a prime and a is an integer such that $p \nmid a$, then $a^{p-1} \equiv 1(modp)$.

Lemma: If a and m are relatively prime, then the least residues of $a, 2a, 3a, ..., (m-1)a(modm)$ are equivalent to $1, 2, 3, ..., (m-1)(modm)$.

Proof: Let p be a prime and $a \in \mathbb{Z}$ such that $p \nmid a$. By definition of "relatively prime," $(a, p) = 1$. Thus, by the Lemma mentioned above, $a, 2a, 3a, ..., (p-1)a(modp)$ have the least residues of $1, 2, 3, ..., p-1(modp)$ up to reordering. Hence,

$$\begin{aligned} a \cdot 2a \cdot 3a...(p-1) \cdot a &\equiv 1 \cdot 2 \cdot 3 \cdot ...(p-1)(modp) \\ &\equiv (p-1)! \\ &\equiv -1(modp) \quad \text{By Wilson's Theorem} \end{aligned}$$

Note that $a \cdot 2a \cdot 3a...(p-1) \cdot a = a^{p-1} \cdot (p-1)!)$.

Thus, $a^{p-1} \cdot (p-1)! \equiv a^{p-1} \cdot (-1) \equiv (-1)(modp)$.

By definition of multiplicative inverse, $(-1)^{-1} \equiv (-1)(modp) \equiv (p-1)(modp)$. Hence,

$$\begin{aligned} a^{p-1} &\equiv (-1) \cdot a^{p-1} \cdot (-1) \\ &\equiv (-1) \cdot (-1) \\ &\equiv 1(modp) \end{aligned}$$

####Primality Test If $n \in \mathbb{Z}^+$, $n > 1$, and n has no prime divisor p with $p \leq \sqrt{n}$, then n is a prime.

Once two primes are found, multiplying them together yields n, the modulus used in each of the key pairs. The reason for doing this is to try to create what is known as a "trapdoor function." In most simple terms, a trapdoor function is a function that easily goes in one direction, but going backwards (the inverse of the function) is more difficult.

For example, say the two prime numbers I picked were 257 and 331. Then, computing $n = (257)(331) = 85,067$ takes no time at all. Now consider going the other direction. If I gave you the product, 85,067 to begin with and asked you to find the two primes I multiplied together, then this process would take much longer. Going one direction was easy, but going the other direction was much more difficult. The same difficulty goes for computers. This is the beauty of RSA encryption. Algorithms can be ranked by their efficiency. In the example above, 257 and 331 are incredibly small primes relative to the primes used for RSA encryption. Multiplying two of these large numbers still takes a small amount of time and resources. However, factoring n is an incredibly lengthy process to figure out the keys. In fact, recovering a prime number of 1024 bits would require a years worth of work on $10 million machine, and recovering a prime number of 2048 bits would require several billion times more work.[2] However, this process is possible due to the "Unique Factorization Theorem." The prime factorization of 1024 bit number (308 digits) may still be an incredibly long factorization.

Unique Factorization Theorem

Every natural number $n > 1$ can be uniquely expressed as a product of primes.

i.e. $n = (p_1^{e_1})(p_2^{e_2})(p_3^{e_3})...(p_k^{e_k})$ for distinct primes p_i and positive integers e_i with $1 \leq i \leq k$.

#Idea: include a really big number

##Euler's Totient Function
Euler's Totient function is relatively simple. For any positive integer, n, $\phi(n)$ is the sum of all the positive divisors of n denoted as:

$$\phi(n) = \sum_{d|n} d$$

Next Generation in Encryption Standards

Because of advancements in computer technology, the next generation of encryption standards is currently under consideration by the National Institute of Standards and Technology ("NIST").

NIST

The NIST is the premier, standard-setting organization in the U.S. According to its website, the mission of the NIST is to "promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life." Originally founded in 1901, the NIST is a part of the U.S. Department of Commerce and has led the promulgation of encryption standards. NIST technology secures tablets, cellphones, and ATMs; encrypts international transactions on the web; and protects US federal information including those with national security implications.

NIST's first encryption standard was known as the Data Encryption Standard (DES) and was adopted in 1977. The DES standard, its definition, and processing standards were withdrawn in 2005. The NIST published its second standard, the Advanced Encryption Standard (AES), in 1997 after a 4 1/2-year process. The AES was officially adopted in 2001. The encryption algorithm is known as the "Rijndael" algorithm and was developed by Belgium scientists Joan Daemen and Vincent Rijmen. (The algorithm is pronounced as "rain doll"). The Rijndael algorithm was picked as the best out of the 15 originally submitted algorithms. NIST is in the process of adopting its third standard because of advances in quantum computing.

Quantum Computing

Quantum computing is the next generation in computer technology and harnesses the power of quantum mechanics. According to wikipedia, "while quantum computers provide no additional advantages over classical computers in terms of computability, quantum algorithms for certain problems have significantly lower time complexities than corresponding known classical algorithms. Notably, quantum computers are believed to be able to quickly solve certain problems that no classical computer could solve in any feasible amount of time—a feat known as"quantum supremacy."

NIST's annual report, "2021 Cybersecurity and Privacy Annual Report", described the state of quantum computing and cryptography as follows:

> [T]here has been steady progress in building quantum computers – machines that exploit quantum mechanical phenomena to solve problems that are difficult or intractable for conventional computers. When the capacity to build large-scale quantum computers exists, they will be able to break many of the public-key cryptosystems currently in use. This weakness would seriously compromise the confidentiality and integrity of digital communications online and elsewhere.

An ominous prediction was offered within the report that current public key encryption systems will be obsolete within the next 20 years.

McKinsey and Company releases a quarterly report entitled, "Quantum Technology Monitor." In June 2022, McKinsey documented $1.24 billion in private investment start-ups and $1.9 billion of announced government funding for the development of quantum technology. China increased its quantum technology patent activity and originated more than half globally. "Public and private funding continues to **skyrocket** around the world, with North America still investing the most."

Standardized Algorithm

The next generation of encryption standards is being considered by NIST and deemed a priority because of advances in quantum computing. To meet this new challenge, NIST began by evaluating 15 new algorithms. The algorithms were evaluated in rounds with the third round victors being announced in 2022 and a fourth round to be held for the remaining algorithms. According to the latest news release on July 5, 2022, NIST will recommend for most use cases the CRYSTALS-KYBER for key establishment and CRYSTALS-Dilithium for digital signatures. The current status of the standard is maintained on the NIST Post-Quantum Cryptography Project website.

In describing CRYSTALS-KYBER's performance, the NIST declared the public and cipher key size "in the order of a thousand bytes which should be acceptable for most applications." The conclusion was that "the security of KYBER has been thoroughly analyzed and is based on a strong framework of results in lattice-based cryptography. KYBER has excellent performance overall in software, hardware, and many hybrid settings."

Conclusion

Introduction

"In ancient India, there were two kinds of ciphers Kauitiliyam and Mulavediya noted in 2000 year old Kamasutra of Vatsyayana." (Naser, 2021, p. 12) (pdf)[3]

"The first cipher device was probably invented by Leon Battista Alberti, an automatic cipher device, where he used a wheel." (Naser, 2021, p. 12) (pdf)[3]

References

1. Lefton P (1991) Number Theory and Public-Key Cryptography. *The Mathematics Teacher* 84: 54–63.

2. Jahan I, Asif M, Rozario LJ (2015) Improved RSA cryptosystem based on the study of number theory and public key cryptosystems. *American Journal of Engineering Research (AJER)* 4: 143–149.

3. Naser SM (2021) Cryptography: From The Ancient History to Now, It's Applications and a New Complete Numerical Model,.

Appendix

Table 2: First 500 Primes

2	3	5	7	11	13	17	19	23	29
31	37	41	43	47	53	59	61	67	71
73	79	83	89	97	101	103	107	109	113
127	131	137	139	149	151	157	163	167	173
179	181	191	193	197	199	211	223	227	229
233	239	241	251	257	263	269	271	277	281
283	293	307	311	313	317	331	337	347	349
353	359	367	373	379	383	389	397	401	409
419	421	431	433	439	443	449	457	461	463
467	479	487	491	499	503	509	521	523	541
547	557	563	569	571	577	587	593	599	601
607	613	617	619	631	641	643	647	653	659
661	673	677	683	691	701	709	719	727	733
739	743	751	757	761	769	773	787	797	809
811	821	823	827	829	839	853	857	859	863
877	881	883	887	907	911	919	929	937	941
947	953	967	971	977	983	991	997	1009	1013
1019	1021	1031	1033	1039	1049	1051	1061	1063	1069
1087	1091	1093	1097	1103	1109	1117	1123	1129	1151
1153	1163	1171	1181	1187	1193	1201	1213	1217	1223
1229	1231	1237	1249	1259	1277	1279	1283	1289	1291
1297	1301	1303	1307	1319	1321	1327	1361	1367	1373
1381	1399	1409	1423	1427	1429	1433	1439	1447	1451
1453	1459	1471	1481	1483	1487	1489	1493	1499	1511
1523	1531	1543	1549	1553	1559	1567	1571	1579	1583
1597	1601	1607	1609	1613	1619	1621	1627	1637	1657
1663	1667	1669	1693	1697	1699	1709	1721	1723	1733
1741	1747	1753	1759	1777	1783	1787	1789	1801	1811
1823	1831	1847	1861	1867	1871	1873	1877	1879	1889
1901	1907	1913	1931	1933	1949	1951	1973	1979	1987
1993	1997	1999	2003	2011	2017	2027	2029	2039	2053
2063	2069	2081	2083	2087	2089	2099	2111	2113	2129
2131	2137	2141	2143	2153	2161	2179	2203	2207	2213
2221	2237	2239	2243	2251	2267	2269	2273	2281	2287
2293	2297	2309	2311	2333	2339	2341	2347	2351	2357
2371	2377	2381	2383	2389	2393	2399	2411	2417	2423
2437	2441	2447	2459	2467	2473	2477	2503	2521	2531
2539	2543	2549	2551	2557	2579	2591	2593	2609	2617
2621	2633	2647	2657	2659	2663	2671	2677	2683	2687
2689	2693	2699	2707	2711	2713	2719	2729	2731	2741
2749	2753	2767	2777	2789	2791	2797	2801	2803	2819
2833	2837	2843	2851	2857	2861	2879	2887	2897	2903
2909	2917	2927	2939	2953	2957	2963	2969	2971	2999
3001	3011	3019	3023	3037	3041	3049	3061	3067	3079
3083	3089	3109	3119	3121	3137	3163	3167	3169	3181

Table 2: First 500 Primes *(continued)*

3187	3191	3203	3209	3217	3221	3229	3251	3253	3257
3259	3271	3299	3301	3307	3313	3319	3323	3329	3331
3343	3347	3359	3361	3371	3373	3389	3391	3407	3413
3433	3449	3457	3461	3463	3467	3469	3491	3499	3511
3517	3527	3529	3533	3539	3541	3547	3557	3559	3571

Appendix

Table 3: US-ASCII Printable Characters

DEC	OCT	HEX	BIN	Symbol	HTML Number	HTML Name	Description
32	40	20	100000	NA	&#32;	NA	Space
33	41	21	100001	!	&#33;	NA	Exclamation mark
34	42	22	100010	"	&#34;	&quot;	Double quotes (or speech marks)
35	43	23	100011	#	&#35;	NA	Number
36	44	24	100100	$	&#36;	NA	Dollar
37	45	25	100101	%	&#37;	NA	Per cent sign
38	46	26	100110	&	&#38;	&amp;	Ampersand
39	47	27	100111	’	&#39;	NA	Single quote
40	50	28	101000	(	&#40;	NA	Open parenthesis (or open bracket)
41	51	29	101001	)	&#41;	NA	Close parenthesis (or close bracket)
42	52	2A	101010	*	&#42;	NA	Asterisk
43	53	2B	101011	+	&#43;	NA	Plus
44	54	2C	101100	,	&#44;	NA	Comma
45	55	2D	101101	-	&#45;	NA	Hyphen
46	56	2E	101110	.	&#46;	NA	Period, dot or full stop
47	57	2F	101111	/	&#47;	NA	Slash or divide
48	60	30	110000	0	&#48;	NA	Zero
49	61	31	110001	1	&#49;	NA	One
50	62	32	110010	2	&#50;	NA	Two
51	63	33	110011	3	&#51;	NA	Three
52	64	34	110100	4	&#52;	NA	Four
53	65	35	110101	5	&#53;	NA	Five
54	66	36	110110	6	&#54;	NA	Six
55	67	37	110111	7	&#55;	NA	Seven
56	70	38	111000	8	&#56;	NA	Eight
57	71	39	111001	9	&#57;	NA	Nine
58	72	3A	111010	:	&#58;	NA	Colon
59	73	3B	111011	;	&#59;	NA	Semicolon
60	74	3C	111100	<	&#60;	&lt;	Less than (or open angled bracket)
61	75	3D	111101	=	&#61;	NA	Equals
62	76	3E	111110	>	&#62;	&gt;	Greater than (or close angled bracket)
63	77	3F	111111	?	&#63;	NA	Question mark
64	100	40	1000000	@	&#64;	NA	At symbol
65	101	41	1000001	A	&#65;	NA	Uppercase A
66	102	42	1000010	B	&#66;	NA	Uppercase B
67	103	43	1000011	C	&#67;	NA	Uppercase C
68	104	44	1000100	D	&#68;	NA	Uppercase D
69	105	45	1000101	E	&#69;	NA	Uppercase E
70	106	46	1000110	F	&#70;	NA	Uppercase F
71	107	47	1000111	G	&#71;	NA	Uppercase G
72	110	48	1001000	H	&#72;	NA	Uppercase H
73	111	49	1001001	I	&#73;	NA	Uppercase I
74	112	4A	1001010	J	&#74;	NA	Uppercase J
75	113	4B	1001011	K	&#75;	NA	Uppercase K

Table 3: US-ASCII Printable Characters *(continued)*

DEC	OCT	HEX	BIN	Symbol	HTML Number	HTML Name	Description
76	114	4C	1001100	L	&#76;	NA	Uppercase L
77	115	4D	1001101	M	&#77;	NA	Uppercase M
78	116	4E	1001110	N	&#78;	NA	Uppercase N
79	117	4F	1001111	O	&#79;	NA	Uppercase O
80	120	50	1010000	P	&#80;	NA	Uppercase P
81	121	51	1010001	Q	&#81;	NA	Uppercase Q
82	122	52	1010010	R	&#82;	NA	Uppercase R
83	123	53	1010011	S	&#83;	NA	Uppercase S
84	124	54	1010100	T	&#84;	NA	Uppercase T
85	125	55	1010101	U	&#85;	NA	Uppercase U
86	126	56	1010110	V	&#86;	NA	Uppercase V
87	127	57	1010111	W	&#87;	NA	Uppercase W
88	130	58	1011000	X	&#88;	NA	Uppercase X
89	131	59	1011001	Y	&#89;	NA	Uppercase Y
90	132	5A	1011010	Z	&#90;	NA	Uppercase Z
91	133	5B	1011011	[	&#91;	NA	Opening bracket
92	134	5C	1011100	\	&#92;	NA	Backslash
93	135	5D	1011101	]	&#93;	NA	Closing bracket
94	136	5E	1011110	^	&#94;	NA	Caret - circumflex
95	137	5F	1011111	_	&#95;	NA	Underscore
96	140	60	1100000	‘	&#96;	NA	Grave accent
97	141	61	1100001	a	&#97;	NA	Lowercase a
98	142	62	1100010	b	&#98;	NA	Lowercase b
99	143	63	1100011	c	&#99;	NA	Lowercase c
100	144	64	1100100	d	&#100;	NA	Lowercase d
101	145	65	1100101	e	&#101;	NA	Lowercase e
102	146	66	1100110	f	&#102;	NA	Lowercase f
103	147	67	1100111	g	&#103;	NA	Lowercase g
104	150	68	1101000	h	&#104;	NA	Lowercase h
105	151	69	1101001	i	&#105;	NA	Lowercase i
106	152	6A	1101010	j	&#106;	NA	Lowercase j
107	153	6B	1101011	k	&#107;	NA	Lowercase k
108	154	6C	1101100	l	&#108;	NA	Lowercase l
109	155	6D	1101101	m	&#109;	NA	Lowercase m
110	156	6E	1101110	n	&#110;	NA	Lowercase n
111	157	6F	1101111	o	&#111;	NA	Lowercase o
112	160	70	1110000	p	&#112;	NA	Lowercase p
113	161	71	1110001	q	&#113;	NA	Lowercase q
114	162	72	1110010	r	&#114;	NA	Lowercase r
115	163	73	1110011	s	&#115;	NA	Lowercase s
116	164	74	1110100	t	&#116;	NA	Lowercase t
117	165	75	1110101	u	&#117;	NA	Lowercase u
118	166	76	1110110	v	&#118;	NA	Lowercase v
119	167	77	1110111	w	&#119;	NA	Lowercase w
120	170	78	1111000	x	&#120;	NA	Lowercase x
121	171	79	1111001	y	&#121;	NA	Lowercase y

Table 3: US-ASCII Printable Characters *(continued)*

DEC	OCT	HEX	BIN	Symbol	HTML Number	HTML Name	Description
122	172	7A	1111010	z	&#122;	NA	Lowercase z
123	173	7B	1111011	{	&#123;	NA	Opening brace
124	174	7C	1111100	|	&#124;	NA	Vertical bar
125	175	7D	1111101	}	&#125;	NA	Closing brace
126	176	7E	1111110	~	&#126;	NA	Equivalency sign - tilde
127	177	7F	1111111	NA	&#127;	NA	Delete

Appendix - Encrypt Number Using RSA

This is a short RSA encryption example taken from Chapter 5.3. RSA Public Key Cryptography, Introduction to Cryptography by Gary Kessler. To encrypt a message, the receiver generates two public keys n and e, and one private key d.

Step 1.

Choose two prime numbers, p and q. From these numbers you can calculate the modulus, $n = pq$.

```
p <- 3; q <- 5
n <- p * q
```

Step 2.

Select a third number, e, that is relatively prime to (i.e., it does not divide evenly into) the product $(p-1)(q-1)$. The number e is the public exponent. $(p-1) * (q-1) = 8$, so choose 11.

```
e <- 11
```

Step 3.

Calculate an integer d from the quotient $(ed-1)/[(p-1)(q-1)]$. The number d is the private exponent.

```
d <- 3
```

Step 4.

Compose a message M. Here, the message consists of a single integer "7".

```
M <- 7
```

Step 5.

Encrypt message to cipher text C with the equation, $C = M^e \mod n$.

```
(C <- (M^e) %% n)
```

```
## [1] 13
```

Step 6.

The receiver decrypts the ciphertext C using the private key value $(d, n) = (3, 15)$.

```
(C^d) %% n
```

```
## [1] 7
```