

Harold's Cryptology Cheat Sheet

9 September 2025

Definitions

Term	Definition
Cryptology	The study of cryptography and cryptanalysis
Cryptography	Methods of encipherment (secret techniques)
Cryptanalysis	Methods of decipherment (code breaking)
Plain	Plain text message to be encrypted
Cipher	Encrypted text message to be decrypted
Key	Secret string or set of numbers used to encrypt plain text
Steganography	Information hiding in files, like JPG images

Text to Numbers Encoding

Letter	Number	Letter	Number
A	00	N	13
B	01	O	14
C	02	P	15
D	03	Q	16
E	04	R	17
F	05	S	18
G	06	T	19
H	07	U	20
I	08	V	21
J	09	W	22
K	10	X	23
L	11	Y	24
M	12	Z	25
		<space>	26

Cipher Methods

Method	Concept	Example	How
Shift	m = plain text message c = cipher text e.g., ("A" = 0, "B" = 1, ...) $0 \leq a, b < n$ $\gcd(a, n) = 1$ (coprime)		Modular Arithmetic for all three (see Harold's Modular Arithmetic Cheat Sheet)
	Multiply and shift, then wrap	Affine Ciphers	$c = (am + b) \text{ MOD } n$ $m = (a^{-1}(c - b)) \text{ MOD } n$ To find a^{-1} , solve for r : $(c - b) \cdot r \equiv 1 \pmod{n}$ Since $r = a^{-1}$, then $a^{-1}am = m \pmod{n}$
	Shift and wrap	Caesar Cipher	$c = (m + b) \text{ MOD } n$ $m = (c - b) \text{ MOD } n$ Same as Affine with $a = 1$.
	Multiply and wrap	Decimation Cipher	$c = (am) \text{ MOD } n$ Same as Affine with $b = 0$ and "A" = "A".
Substitution	Replacement (simple)	Mixed Alphabet with Key Words	Key: Unique letters of the key word in order, without repetitions Plain: A B C ... X Y Z Cipher: <Key> followed by remaining letters of the alphabet, without repetitions
		Keyword Columnar Transposition Substitution	1. Row 1: Key word unique chars (# cols) 2. Rows 2-n: Remaining unique chars in rows of a fixed column table 3. Add a padding character as needed 4. Cipher text is simply reading columns top down in alphabetical order
Transposition	Rearranged	Columnar Transposition	1. Agree upon number of columns 2. Rows 1-n: Use clear text to write out rows of a fixed column table 3. Add a padding character as needed 4. Cipher text is simply reading columns top down in order left to right

Spreadsheet Example – Caesar Cipher

Function	Description					Excel Formula																																																																
<table><tr><th>Operation</th><th></th><th>A</th><th>B</th><th>C</th><th>D</th><th>E</th><th>F</th><th>G</th><th>H</th><th>I</th><th>J</th></tr><tr><td>Plain Text</td><td>1</td><td>S</td><td>K</td><td>Y</td><td>I</td><td>S</td><td>C</td><td>L</td><td>E</td><td>A</td><td>R</td></tr><tr><td>Plain Text as #</td><td>2</td><td>18</td><td>10</td><td>24</td><td>8</td><td>18</td><td>2</td><td>11</td><td>4</td><td>0</td><td>17</td></tr><tr><td>Cipher Text as #</td><td>3</td><td>25</td><td>27</td><td>5</td><td>15</td><td>25</td><td>9</td><td>18</td><td>11</td><td>7</td><td>24</td></tr><tr><td>Cipher Text</td><td>4</td><td>Z</td><td>R</td><td>F</td><td>P</td><td>Z</td><td>J</td><td>S</td><td>L</td><td>H</td><td>Y</td></tr></table>											Operation		A	B	C	D	E	F	G	H	I	J	Plain Text	1	S	K	Y	I	S	C	L	E	A	R	Plain Text as #	2	18	10	24	8	18	2	11	4	0	17	Cipher Text as #	3	25	27	5	15	25	9	18	11	7	24	Cipher Text	4	Z	R	F	P	Z	J	S	L	H	Y
Operation		A	B	C	D	E	F	G	H	I	J																																																											
Plain Text	1	S	K	Y	I	S	C	L	E	A	R																																																											
Plain Text as #	2	18	10	24	8	18	2	11	4	0	17																																																											
Cipher Text as #	3	25	27	5	15	25	9	18	11	7	24																																																											
Cipher Text	4	Z	R	F	P	Z	J	S	L	H	Y																																																											
CODE("A")	Converts an ASCII character into a number					A2=CODE (A1) - CODE ("A")																																																																
MOD(n, m)	Adds a fixed offset to each number (n) then mods it by m					A3=MOD (A2 + 7, 26)																																																																
CHAR(65)	Converts a number into an ASCII character					A4=CHAR (A3 + CODE ("A"))																																																																
Combined	All three functions combined into one					A4=CHAR (MOD (CODE (A1) - CODE ("A") + 7, 26) + CODE ("A"))																																																																

Frequency Analysis

Language	Combos	Letter Frequency
English	Letters	ETOANIS RHCUL ETAOI NSHRD LCUMW FGYPB VKXJQZ (Texts) ESIAR NTOLC DUGPM HBYFV KWZXXJQ (Dictionaries) ETAON RISHD LFCMU GYPWB VKJXZQ (40K sample) ETAOI NSRHD LUCMF YWGPB VKXQJZ ETAOI NSRHL DCUMF PGWYB VKXJQZ
	Diagrams	TH HE AN RE ER IN ON AT ND ST ES EN OF TE ED OR TI HI AS TO TH HE IN EN NT RE ER AN TI ES ON AT SE ND OR AR AL TE CO DE TO RA ET ED IT SA EM RO
	Double Letters	LL EE SS OO TT FF RR NN PP CC
	Trigrams	THE AND THA ENT ING ION TIO FOR NDE HAS NCE EDT TIS OFT STH MEN
	Words	1500 Most Commonly Used English Words in Daily Life
French	Letters	ESAIT NRUOL DCMFV ÉQFBG HJÀXZ ÈÊYÇK ÛÛÂW
Italian	Letters	EAION LRTSC DPUMV GZFBH ÀQÈÚW ÍYJKX ÒÈÇÆ
German	Letters	ENSRI ATDHU LGCOM WBFKZ ÜÖßJY XQÀÈÚ ÍÒÉ
Spanish	Letters	EAOSR NIDLC TUMPB GYÍVQ ÓHFZJ ÉÁÑXÚ ÜWK

RSA Algorithm

Term	Definition	
RSA	Public key cryptosystem developed by Rivest, Adelman, and Shamir in 1978.	
Key Prep	- Bob selects two large prime numbers, p and q. - Bob computes $N = pq$ and $\phi = (p-1)(q-1)$ - Bob finds an integer e such that $\gcd(e, \phi) = 1$. - Bob computes the multiplicative inverse of $e \bmod \phi$: an integer d such that $(ed \bmod \phi) = 1$. - Public (encryption) key: N and e. - Private (decryption) key: d.	
Example	- Bob selects two primes: $p = 31$ $q = 59$ - Compute: $N = p \cdot q = 31 \cdot 59 = 1829$ $\phi = (p - 1) \cdot (q - 1) = 30 \cdot 58 = 1740$ - Find integer e such that $\gcd(e, \phi) = 1$ Guess $e = 859$ and check: $\gcd(859, 1740) = 1$ If the first guess is not relatively prime to ϕ, try another. - Using Euclid's algorithm, find A and B such that $A \cdot 859 + B \cdot 1740 = 1$ $79 \cdot 859 + (-39) \cdot 1740 = 1$ $79 \cdot 859 = 1 \bmod 1740$ $d = 79$ is the inverse of $859 \bmod 1740$ - Public key: (e, N) $e = 859$ $N = 1829$ - Private key: (d, N) $d = 79$ $N = 1829$	
Encryption	$c = m^e \bmod N$	Public key: 
Decryption	$m = c^d \bmod N$	Private key: 
Number Theory Fact	Let p and q be prime numbers and $pq = N$. Suppose that $m \in \mathbb{Z}_N$ and $\gcd(m, N) = 1$. Then $m^{(p-1)(q-1)} \bmod N = 1$.	
Theorem: Validity of the RSA Cryptosystem	If $m \in \mathbb{Z}_N$ and $\gcd(m, N) = 1$, then RSA encryption and decryption applied to m always yield m as the unique result.	

Sources:

- [SNHU MAT 230](#) - Discrete Mathematics, zyBooks.
- [SNHU MAT 260](#) - Cryptology, [Invitation to Cryptology](#), 1st Edition, Thomas Barr, 2001.