**Harold’s Cryptology Cheat Sheet**

17 December 2022

**Definitions**

|  |  |
| --- | --- |
| **Term** | **Definition** |
| **Cryptology** | The study of cryptography and cryptoanalysis |
| **Cryptography** | Methods of encipherment (secret techniques) |
| **Cryptoanalysis** | 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 |
| **Stegenography** | 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, ...) | | Modular Arithmetic for all three (see Harold’s Modular Arithmetic Cheat Sheet) |
| Multiply and shift, then wrap | **Affine Ciphers** | To find *a*-1, solve for *r*:  Since ,  then |
| Shift and wrap | **Caesar Cipher** | Same as Affine with *a* = 1. |
| Multiply and wrap | **Decimation Cipher** | 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** |
| |  |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | **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** |
| Chart, bar chart, histogram  Description automatically generated | | |
| **English** | Letters | ETOANIS RHCUL  ETAOI NSHRD LCUMW FGYPB VKXJQZ (Texts)  ESIAR NTOLC DUGPM HBYFV KWZXJQ (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 |
| **French** | Letters | ESAIT NRUOL DCMPV ÉQFBG HJÀXZ ÈÊYÇK ÛÙÂW |
| **Italian** | Letters | EAION LRTSC DPUMV GZFBH ÀQÈÚW ÍYJKX ÒÉÇÆ |
| **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** | 1. Bob selects two large prime numbers, p and q. 2. Bob computes N = pq and φ = (p-1) (q-1) 3. Bob finds an integer e such that gcd (e, φ) = 1. 4. Bob computes the multiplicative inverse of e mod φ: an integer d such that (ed mod φ) = 1. 5. Public (encryption) key: N and e. 6. Private (decryption) key: d. | |
| Example | 1. Bob selects two primes:  p = 31  q = 59  2. Compute:  N = p ⋅ q = 31 ⋅ 59 = 1829  ϕ = (p - 1) ⋅ (q - 1) = 30 ⋅ 58 = 1740  3. Find integer e such that gcd (e, ϕ) = 1  Guess e = 859 and check: gcd (859, 1740) = 1  If the first guess is not relatively prime to ϕ, try another.  4. Using Euclid's algorithm, find A and B such that A ⋅ 859 + B ⋅ 1740 = 1  79 ⋅ 859 + (-39) ⋅ 1740 = 1  79 ⋅ 859 = 1 mod 1740  d = 79 is the inverse of 859 mod 1740  5. Public key: (e, N)  e = 859  N = 1829  6. Private key: (d, N)  d = 79  N = 1829 | |
| **Encryption** |  |  |
| **Decryption** |  |  |
| **Number Theory Fact** | Let p and q be prime numbers and pq = N.  Suppose that m ∈ **Z**N and gcd (m, N) = 1.  Then m(p-1)(q-1) mod N = 1. | |
| **Theorem: Validity of the RSA Cryptosystem** | If m ∈ **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](https://www.snhu.edu/admission/academic-catalogs/coce-catalog#/courses/4kVhSZLtg) - Discrete Mathematics, zyBooks.
* [SNHU MAT 260](https://www.snhu.edu/admission/academic-catalogs/coce-catalog#/courses/NkdqI-8Fe) - Cryptology, I[nvitation to Cryptology](https://www.amazon.com/Invitation-Cryptology-Thomas-H-Barr/dp/0130889768/ref=sr_1_1?crid=9A8O5P2JQ7F&keywords=978-0-13-088976-8&qid=1656057152&sprefix=978-0-13-088976-8%2Caps%2C71&sr=8-1), 1st Edition, Thomas Barr, 2001.