

Mathematica Command Reference Sheet

Note: Commands that start with an upper case letter are built-in commands. Commands that start with a lower case letter are user-defined commands which will require you to evaluate the initialization cell in the corresponding notebook.

JBA01IntroductionGCD.nb

- `GCD[a,b]` - computes the greatest common divisor of a and b .
- `PrimeQ[n]` - returns “True” if n is prime and “False” if n is not prime.
- `Prime[n]` - computes the n -th prime number.

JBA02ModularArithmetic

- `Mod[a,b]` - computes the remainder when a is divided by b .
- `toNumbers[text]` - converts a string of text to a list of numbers. Note: the text must be enclosed in quotation marks.
- `toLetters[list]` - converts a list of numbers to a string of text.

JBA03AffineCiphers.nb

JBA04Cryptanalysis.nb

- `analyze[text]` - performs a frequency count on the text and computes a number of other useful cryptanalysis quantities,
- `showDigraphs[n]` - lists the top n digraphs in the text being analyzed. Note: you must run the analyze command on the text before using this command.
- `showTrigraphs[n]` - lists the top n trigraphs in the text being analyzed. Note: you must run the analyze command on the text before using this command.
- `showLetters` - Lists the letters and corresponding frequencies of the text being analyzed in order of most frequent to least frequent. Note: you must run the analyze command on the text before using this command.
- `showFreqs` - Lists the letters and corresponding relative frequencies of the text being analyzed in order of most frequent to least frequent. Note: you must run the analyze command on the text before using this command.

JBA05Vigenere.nb

- `vig[m,k]` - enciphers the message m using the Vigenere cipher with keyword k . Both m and k must be in quotes.
- `devig[m,k]` - decipheres the message m using the Vigenere cipher with keyword k . Both m and k must be in quotes.
- `showQuadgraphs[n]` - lists the top n quadgraphs in the text being analyzed. Note: you must run the analyze command on the text before using this command.
- `submessage[m,a,b]` - extracts the submessage from m which begins with the a -th letter and takes every b -th letter after.

JBA06OnetimePad.nb

- `onetime[n]` - creates a random string of letters of length n .

JBA07Matrices.nb

- `Inverse[A]` - computes the matrix inverse of the matrix A , if it exists.

JBA08HillCipher.nb

- `toPairsOfNumbers [text]` - converts a string of text to a list of pairs of numbers given as a matrix with two rows.
- `fromPairsOfNumbers [text]` - converts a list of pairs of numbers given in as a matrix with two rows to a string of text.
- `hill [m,a,b,c,d]` - uses the Hill cipher to encipher the message m with the matrix $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ as the key.
- `matrixInverseMod26 [a,b,c,d]` - computes the inverse of the matrix $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \pmod{26}$.

JBA09HillCipherCryptanalysis.nb

- `matrixSolve [A,b]` - finds solutions to the matrix equation $Ax = b$ for $x \pmod{26}$.
- `dehill [m,a,b,c,d]` - decipheres a message m which has been enciphered using the Hill cipher with the matrix $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ as the key.

JBA10PowersModp.nb

- `PowerMod [a,k,n]` - computes $a^k \pmod{n}$.

JBA11PohligHellman.nb

- `toQuadgraphNumbers [text]` - converts a string of text to numbers and combines numbers every four numbers into a single number.
- `fromQuadgraphNumbers [list]` - the reverse of the `toQuadgraphNumbers` command.

JBA12Binary.nb

- `toBinary [text]` - converts a string of text to ASCII and
- `fromBinary [list]` - converts a list of 8 bit strings back
- `binaryAdd [l,b]` - converts l to a list of binary strings the
- `binaryToCipherLetters [l]` - converts a list of binary strings to a string of text.
- `cipherLettersToBinary8Bit [m]` - reverses the the `binaryToCipherLetters` command returning a list of 8 bit strings.

JBA13OnetimePads

- `randomPowers [p,b,t,1]` - computes l powers of $b \pmod{p} \pmod{2}$ starting at k .
- `cipherLettersToBinary [text]` - reverses the the `binaryToCipherLetters` command returning a single binary string.

JBA14DiffieHellman.nb

- `dhEncrypt [m,k]` - encrypts the message m using the Diffie-Hellman algorithm with key k .
- `dhDecrypt [c,k]` - decrypts the ciphertext c which has been encrypted using the Diffie-Hellman algorithm with key k .

JBA15RSA.nb

- `nextprime[n]` - returns the smallest prime number greater than or equal to n .
- `rsaEncrypt[m,t,n]` - encrypts the message m using the RSA algorithm with public exponent t and modulus n .
- `rsaDecrypt[c,t,p,q]` - decrypts the ciphertext c which has been encrypted using the RSA algorithm with key public exponent t and prime factors p and q of the modulus n .