JScrypt

Global

compareKey
generateRandomSalt
getComponents
hashKey

Methods

compareKey(cleanKey, hashKey) → {Boolean}

Hashes the cleanKey provided as input and compares the hashed string to the haskKey provided as input. If both values match, returns true, otherwise the function returns false.

Parameters:

Name	Type	Description
cleanKey	String	Plain text password that the user wants to compare to hashed password.
hashKey	String	Corresponding hashed password.

Source: JScrypt.js, line 153

generateRandomSalt(rounds) → {String}

Generates a random padded string of length 24, which is used for hashing the key. This string includes padding which later will be removed before hashing the key.

Parameters:

Name	Type	Description
rounds	Integer	Number of time the key is hashed.

Source: JScrypt.js, line 41

Returns:

Random padded string of length 24.

Type
String

getComponents(hashKey) → {Array}

Parses the input hashKey and returns its various components in an array.

Parameters:

Name	Type	Description
hashKey	String	String input of length 1 to 56.

Source: JScrypt.js, line 208

Returns:

Array of components that have been parsed from the haskKey.

Type
Array

hashKey(rounds, key) → {String}

Generates the hash string that will be stored in the applications database. This is one of the only two functions that a user of the project will be required to call in their application.

Parameters:

Name	Type	Description
rounds	Integer	Number of time the key is hashed.
key	String	String input of length 1 to 56

Source: JScrypt.js, line 78

Returns:

Encrypted string with various components and random ASCII characters.

Type
String

EksBlowfish

Global

feistel_cipher
feistel_F
keyExpansion

Methods

feistel_cipher(xl, xr) → {String}

The heart of the encryption. Runs through a feistel network 2^rounds number of times at each iteration, the P_arrays and S_boxes are updated according to the salt and the key feistel Network.

Parameters:

Name	Type	Description
xl	string	the left 32 bits of the 64 bit input into the feistel network
xr	string	= the right 32 bits of the 64 bit input into the feistel network

Source: eksBlowfish.js, line 377

Returns:

xl_xr an array containing the new xl and xr values.

Type
String

feistel_F(xl) → {Number}

Helper function of the Feistel_ciph

Parameters:

Name	Type	Description
xl	string	

Source: eksBlowfish.js, line 411

Returns:

returns a number derived from the cipher function using s_boxes.

Type
Number

keyExpansion(salt, key)

Sets up the encryption environment with the given key by setting up the P_arrays and the S_boxes with hexadecimal values of the key. Provides no output.

Parameters:

Name	Type	Description
salt	string	22 character string in base64 as the salt
key	string	1 - 56 character key to be encrypted

Source: eksBlowfish.js, line 296