NUEVAS dudas

Preguntarle por el método calculateDistanceBits de la clase generarClaves

Dejo que pueda ser publica e = privada d?

//Preguntar cual queremos que sea el maximo de nnc a imprimir, ojo con el keySize //Preguntar/calcular por el keySize maximo con el q se calcularan los nnc

//añadir a la info de los ataques el enlace a criptored?

ATAQUE PARADOJA DEL CUMPLEAÑOS

Ataque por paradoja del cumpleaño, Como hacer para comprobar que exponente y modulo están bien metidos manualmente?

Actualmente la paradoja del cumpleaños se calcula calculando los valores iniciales para la columna i y la columna j. para comparar los sucesivos valores de la columna i con el valor inicial de la columna j.

Se puede dar el caso de que se llegue a la mitad contraria del modulo y no se haya producido una colision? Si es asi que hago?

Como sabe legion RSA cual es la clave privada?

Para que sirve? w\*s + e\*t = 1 (en mod e y en mod w) después Se comprueba que w\*s + e\*t = 1

CIFRADO DESCIFRADO FIRMA Y COMPROBACION DE LA FIRMA

No se añade la posibilidad de abrir un archivo guardado en disco porque de abrirse que se leería? Solo la primera línea? Y si hay mas? Que caracteres permitidos, ascii?

Como quiere que sea la firma y cifrado para texto? Ascii? Mas relleno? Como!