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!

contenido de los tooltips.

RAMIO - falta la logica de cuando es texto y añadir la info de cuando es texto

ramio - no se han hecho logs.html de los ataques

ramio - ataques siempre imprimir todos los resultados. Por ejemplo ciclico si es muy grande el num de bits(40) puede que llene el buffer de memoria del textArea

702136613538677073862961839 buen modulo para factorizar

LO que me queda

//Paradox atacks tiene algunos comentarios que despues de hablar se han de quitar

//mirar miller porque falla

Texto cifra y firma. Tb CRT.

Mirar si se pueden cambiar los shortcuts de ayuda en el propio fxml para quitar los control de ayuda.

-Ayuda modelo FlujoLab y contextual. http://www.criptored.upm.es/software/sw\_m001m.htm

-Poner un hiperlink en donde las preferencias para que te lleve a la pagina de github.

Banco de pruebas.

Ejemplos raros-> cuando esta todo en blanco.

Ejemplo Práctico-> como ayuda dentro del programa.http://www.criptored.upm.es/software/sw\_m001c.htm

--CORREO

Hola Jorge,

Gracias por los ejemplos.

En cuanto a la clave privada se realiza gracias a un método de la

clase BigInteger, pero podria crear un método para que se hiciera por

el algoritmo extendido de euclides para claves pequeñas y que a su vez

sacará un log entendible (educativamente hablando).

Perfecto, estarìa muy bien.

Limitarlo a un tamaño lógico, por ejemplo de primos p y q de hasta tres dígitos.

Y en cuanto a la exponenciaciónsucede lo mismo, se realiza gracias a

un método de la clase BigInteger. Pero en este caso, ya programé un

metodo que realizase los calculos del AER, por lo tanto solo sería

añadirle el log.

Lo mismo.

Espero poder irte comentando avances de la interfaz gráfica durante la

semana que viene.

Un saludo.

Saludos

---

RODRIGO DIAZ ARROYO

Universidad Politécnica de Madrid

El 28-02-2017 09:24, Jorge Ramió Aguirre escribió:

Si no recuerdas los algoritmos AEE y AER, además de mi libro

electrónico, los tienes aquí:

<https://www.youtube.com/watch?v=D289EF58Yrw>

<https://www.youtube.com/watch?v=D289EF58Yrw>

Saludos

El 2017-02-28 09:14, Jorge Ramió Aguirre escribió:

Hola Rodrigo.

TE adjunto este ejemplo.

Por cierto, ¿cómo se calcula internamente la clave inversa? ¿Con el AEE?

Lo digo porque en ese caso sería interesante que lo entregase como un log.

Lo mismo digo cuando hace la exponenciación N^e mod n o N^d mod n (que

se puedan hacer por separado porfa). ¿Lo hace con el algoritmo de

exponenciación rápida?

Los dos están en este documento

Saludos