Clase BigInteger

Usar el constructor problablePrime el cual dice que el numero elegido tiene una probabilidad de ser compuesto que no excede 2-100. Ó usar el constructor BigInteger expresando la certeza que queremos que consiga la cual excederá de 1 – 1/2certeza.(o lo que es lo mismo 1-2 -certeza).

Si pides que se genere una clave de manera automática, ¿quieres saber los primos p y q? Si es así, quieres que p y q tengan el mismo numero de bits? No,no? Cuantos bits quieres que tenga uno y que tenga otro? Maxima diferencia entre ambos según num de bits?

cuando se generan las claves automáticamente, la clave publica que numero de bits quieres que tenga? Quieres que se de la opción para 65537?

A nivel de teoría dada en Fundamentos de Seguridad, que importancia hay en las claves publicas parejas?

Se recomendaran primos seguros? O se ignoran en esta aplicación?

Como hacemos con los NNC, los calculamos siempre que se pidan? O por el contrario solo se calculan para números inferiores a X cantidad de bits? Si es asi, que bits o que tiempo ¿ Si siempre que lo pidan vamos a mostrarlos lo metemos en un fichero? Cuantos sacamos máximo por pantalla?

¿Para factorizar N que algoritmo uso para este proyecto? ¿Uso varios? De momento he usado Pollar rho factorizationg

Paradoja del cumpleaños

// comprobar, pero no sirve para nada ((w.multiply(s)).add(publica.multiply(t))).equals(BigInteger.ONE));

NUEVAS dudas

Preguntarle por el método calculateDistanceBits de la clase generarClaves

De cuantos bits hacer que se deje crear la clave automática? A partir de 6 bits ya aparecen claves distintas, pero mejor 8? 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 por paradoja del cumpleaños permitir exponent y modulo que se quiera? Aunque pueda dar lugar a que nunca termine el ataque? Como hacer para comprobar que exponente y modulo están bien metidos manualmente?

ATAQUE PARADOJA DEL CUMPLEAÑOS

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 quiere así o se prefiere que se calcule tb la columna j para comparar con i?

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?

Preguntar a ramio que pasa con legionRSA que no funciona para el valor sacado por pantalla. 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?