MCB Praktikum RSA

VOLG DE ONDERSTAANDE INSTRUCTIES NAUWKEURIG OP!	
Het programma suggereert telkens de juiste bestandsnamen, maar controleer dat altijd wel. Je kunt de bestandsnaam altijd nog wijzigen in het venster dat verschijnt als je op “lees in” of “schrijf weg” hebt gedrukt.	
Alleen de aangevinkte velden worden ingelezen / weggeschreven.	
Om de inhoud van veld A te kopiëren naar veld B: ➢ klik in veld A, de cursor wordt dan zoals hiernaast: ➢ sleep de cursor naar veld B, laat daar de muis los	
ZELF: je eigen naam **ANDER:** de naam van iemand anders	rood: privé / geheim groen: publiek

1. *programma instellen*
   a. klik in het kladblok op de knop RSA
   b. vul je naam in achter **”ZELF”** op de bovenste regel in het kladblok

2. *sleutelpaar maken*
   a. maak willekeurige priemgetallen ***p*** en ***q***, van bijvoorbeeld 100 cijfers, en zet ze in het kladblok
   b. bereken ***n*** (modulus nu leeg laten), en zet hem in het kladblok
   c. bereken ***fi*** = (***p***-1)(***q***-1), en zet hem in het kladblok
   d. kies een willekeurig oneven getal ***e*** (met minder cijfers dan ***n***) als publieke exponent, en zet deze in het kladblok
   e. bereken ***d*** = 1 / ***e*** (mod (***p***-1)(***q***-1)) als privé-exponent, en zet deze in het kladblok
   (als het programma moppert dat dat niet kan moet je een andere ***e*** kiezen)
   f. maak een privé-bestand **ZELF_RSA_PRI.txt** met daarin ***n***, ***e*** en ***d***
   g. maak een publiek bestand **ZELF_RSA_PUB.txt** met daarin ***n*** en ***e*** (maar niet ***d***, ***p***, ***q*** of ***fi***!)

3. *publieke sleutel van iemand anders ophalen*
   a. lees het publieke bestand **ANDER_RSA_PUB.txt** in dat iemand anders heeft gemaakt
   (de waarden van ***n*** en ***e*** in het kladblok vormen nu de publieke sleutel van de ander)
   (de naam van de ander verschijnt onderaan in het kladblok achter **”ANDER”**)

4. *versleutelen*
   a. maak een bericht waarvan het aantal tekens minder dan de helft van het aantal cijfers van ***n*** is (alleen toegestane tekens gebruiken),
   zet het bericht met de Tekst-Getal-omzetter om in een getal ***B***, en zet ***B*** in het kladblok
   b. bereken het geheimschrift ***G***, en zet ***G*** in het kladblok
   c. maak een publiek bestand **voor_ANDER_van_ZELF_RSA_MSG.txt** met alleen ***G***
   (let op: geheime informatie als ***d***, ***p***, ***q***, ***fi*** en ***B*** mag er niet in!)

5. *ontsleutelen*
   a. lees het bestand **ZELF_RSA_PRI.txt** in (je eigen privé-sleutel)
   b. lees een bestand **voor_ZELF_van_ANDER_RSA_MSG.txt** in
   c. ontsleutel het geheimschrift ***G***, en zet het resulterende getal ***B*** in het kladblok
   d. zet het getal ***B*** met de Tekst-Getal-omzetter om in een tekst, als het goed is komt de oorspronkelijke tekst tevoorschijn

Probeer het geheimschrift ***G*** ook eens in tekst om te zetten: komt er iets zinnigs uit?
Kun je een geheimschrift van iemand anders dat niet voor jou bestemd was kraken?
Kun je de privé-sleutel van iemand anders kraken?

6. *handtekening zetten en controleren*
   bedenk nu zelf hoe je een handtekening van jou op een bericht kunt zetten, en hoe je iemand anders er van kunt overtuigen dat dat bericht echt van jouw afkomstig is