MCB Praktikum Diffie-Hellman

VOLG DE ONDERSTAANDE INSTRUCTIES NAUWKEURIG OP, IN DE AANGEGEVEN VOLGORDE!
Voordat je een bestand leest of schrijft, controleer altijd de knop “publiek” / “privé” / “bericht”. Het programma suggereert telkens de juiste bestandsnamen, maar controleer dat altijd wel. Je kunt de bestandsnaam en de directory altijd nog wijzigen in het venster dat verschijnt als je op “lees in” of “schrijf weg” hebt gedrukt, maar doe dat vooral niet.
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: COPY ➢ sleep de cursor naar veld B, laat daar de muis los PASTE

ZELF: je eigen naam **ANDER:** de naam van iemand anders	blauw: systeemparameters, publiek rood: privé / geheim groen: publiek

1. *programma instellen*
   a. klik in het kladblok op de knop DH; de voorgeprogrammeerde systeemparameters ***p***, ***g*** van 50 cijfers verschijnen in het kladblok
   b. vul je naam in achter **”ZELF”** op de bovenste regel in het kladblok

2. *sleutelpaar maken*
   a. neem als privé-sleutel ***x*** een willekeurig getal van 49 cijfers en zet ***x*** in het kladblok (***x*** kun je bijvoorbeeld met behulp van de (Priem)getallenfabriek maken)
   b. bereken de bijbehorende publieke sleutel ***y***, en zet ***y*** in het kladblok
   c. maak een privé-bestand **ZELF_DH_PRI.txt** met daarin ***p***, ***g***, ***y*** en ***x***
   d. maak een publiek bestand **ZELF_DH_PUB.txt** met daarin ***p***, ***g***, en ***y*** (maar niet ***x***!)

3. *sleutels uitwisselen*
   a. als je privé-sleutel ***x*** niet meer in het kladblok staat, lees hem dan in uit het bestand **ZELF_DH_PRI.txt**
   b. lees het publieke bestand **ANDER_DH_PUB.txt** in dat iemand anders heeft gemaakt (deze komt in het kladblok bij ***y****, je eigen privé-sleutel ***x*** en publieke sleutel ***y*** zijn blijven staan; de naam van de ander verschijnt onderaan in het kladblok achter **”ANDER”**)

4. *gedeelde geheim maken*
   a. bereken het gedeelde geheim ***s***, en zet ***s*** in het kladblok
   b. maak een privé-bestand **ZELF_ANDER_DH_GEHEIM.txt** met ***p*** en ***s*** (het is niet erg als hier andere getallen in terecht komen)

5. *versleutelen*
   a. als het gedeelde geheim ***s*** niet meer in het kladblok staat, lees hem dan in uit het bestand **ZELF_ANDER_DH_GEHEIM.txt** (de naam van de ander verschijnt onderaan in het kladblok achter **”ANDER”**)
   b. maak een bericht van maximaal 24 tekens (alleen toegestane tekens gebruiken), zet het bericht met de Tekst-Getal-omzetter om in een getal ***B***, en zet ***B*** in het kladblok
   c. bereken het geheimschrift $G = B \bullet s \pmod p$, en zet ***G*** in het kladblok
   d. maak een publiek bestand **voor_ANDER_van_ZELF_DH_MSG.txt** met alleen ***G*** (let op: geheime informatie als ***x***, ***s*** en ***B*** mag er niet in!)

6. *ontsleutelen*
   a. lees het bestand **ZELF_ANDER_DH_GEHEIM.txt** in
   b. lees het bestand **voor_ZELF_van_ANDER_DH_MSG.txt** in
   c. bereken het getal $B = G / s \pmod p$, en zet ***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 of een gedeeld geheim van iemand anders kraken?