MCRE - Modulaire en Cryptografische Rekenmachine met Elliptische Krommen - Handleiding

1. Inleiding

De MCRE-software is ontwikkeld voor educatief gebruik.

In de eerste plaats bevat de software een *modulaire rekenmachine*, een *(priem)getalfabriek* en een *tekst-getal-omzetter*. Daarmee kunt u onder andere:

- rekenen met hele grote getallen, van vele honderden cijfers, maar wel alleen met gehele getallen;
- modulo-rekenen;
- grote willekeurige getallen maken en grote willekeurige priemgetallen maken;
- leesbare tekst in getallen coderen, en omgekeerd, getallen decoderen tot leesbare tekst.

De software biedt alle bouwstenen die u nodig hebt om zelf enkele cryptografische algoritmen uit te kunnen voeren. Zo kunt u bijvoorbeeld, door dit programma op de goede manier te gebruiken, de volgende dingen doen:

- een RSA-sleutelpaar maken;
- versleutelen en ontsleutelen met RSA:
  - korte teksten in getallen omzetten, en die dan versleutelen met RSA;
  - de versleutelde getallen met RSA ontsleutelen en terugzetten tot de oorspronkelijke teksten;
- digitale handtekeningen maken en controleren:
  - korte teksten in getallen omzetten, en daar dan een handtekening bij maken met RSA;
  - de handtekeningen met RSA controleren op geldigheid;
- een Diffie-Hellman-sleutelpaar maken;
- een gedeeld geheim afspreken:
  - met iemand anders, met wie u alleen afluisterbaar kunt communiceren, een geheim getal maken dat u allebei weet, maar de afluisteraar niet.

Dat gaat allemaal niet vanzelf. U moet de wiskunde achter RSA en Diffie-Hellman eerst bestudeerd hebben, en u moet er wel goed bij nadenken om de juiste stappen te zetten.

Komt u er niet uit, dan kunt u inspiratie opdoen bij een aantal gebruiksvoorbeelden.

De publieke RSA- en Diffie-Hellman-sleutels die u met dit programma maakt kunt u opslaan in bestanden, en dan uitwisselen met anderen die met hetzelfde programma kunnen omgaan. Gebruik hiervoor bijvoorbeeld een USB-stick, e-mail of een chat-programma. Zo kunt u behoorlijk veilig korte berichten uitwisselen.

In de tweede plaats bevat de software drie onderdelen waarmee u enkele andere getaltheoretische algoritmen stap voor stap kunt doorlopen. Het gaat om:

- *Euclides*: het (uitgebreide) algoritme van Euclides voor het bepalen van de grootste gemene deler van twee getallen;
- *Miller*: de primaliteitstest van Miller,

- *Chinese Reststelling*: het oplossen van een stelsel congruentievergelijkingen met de Chinese Reststelling.

2. Handleiding (invul)velden

De invulvelden kunt u bewerken zoals in een gewone editor. Klik in een veld, let op de cursor, en typ cijfers of letters.

U kunt "copy-en-paste" met de muis gebruiken om een getal van het ene veld naar het andere te kopiëren. Dat gaat als volgt:

- klik in het eerste veld en houd de muisknop vast, de cursor verandert dan in de bovenstaande afbeelding,
- verplaats de cursor met ingedrukte muisknop naar het veld van bestemming, en laat daar de muisknop los.

Ook kunt u geselecteerde stukken kopiëren (CTRL-C), knippen (CTRL-X) en plakken (CTRL-V), en kunt u het hele veld selecteren (CTRL-A, of dubbelklik).
Er zijn ook velden waar alleen het programma iets kan zetten. In die velden kunt u niet editen, wel kunt u het hele veld selecteren (CTRL-A, of dubbelklik) en kopiëren (CTRL-C).

U kunt op deze manier met (CTRL-A), (CTRL-C), (CTRL-V) en (CTRL-X) de inhoud van het ene veld naar het andere transporteren. Ook kunt u zo de inhoud verplaatsen van en naar een ander programma, zoals een tekstverwerker, een e-mail-programma of een chatprogramma.

Om getallen tijdelijk op te kunnen slaan bevat het programma een "kladblok", waar u met een enkele muisbeweging getallen naar toe kunt verplaatsen of vandaan kunt halen.
De inhoud van het kladblok kunt u, gedeeltelijk of geheel, ook meteen naar een bestand schrijven, of uit een bestand inlezen.
Deze bestanden gebruiken een voor deze software specifiek formaat. Op die manier kunt u de inhoud (tijdelijk of permanent) bewaren, of uitwisselen met anderen die ook de MCRE-software gebruiken.

Als de inhoud te groot is om in een veld te passen, dan hoeft u niet bang te zijn dat de computer het onzichtbare deel vergeten is. U krijgt de inhoud alleen niet helemaal te zien. Het verborgen deel kunt u te zien krijgen door met de pijltjestoetsen (of met HOME of END) de cursor in het veld ver genoeg naar links of rechts te bewegen.

3. De Modulaire Rekenmachine

Met de *Modulaire Rekenmachine* kunt u *modulair* rekenen (modulo ***m***), en u kunt er ook *gewoon* (niet-modulair) mee rekenen, maar alleen met gehele getallen. U kunt behoorlijk grote getallen gebruiken, zeker tot enkele honderden cijfers groot.

		niet modulair	modulair (mod ***m***)
+	optellen:	$c = a + b$	$c \equiv a + b \pmod m$
-	aftrekken:	$c = a - b$	$c \equiv a - b \pmod m$
×	vermenigvuldigen:	$c = a \times b$	$c \equiv a \times b \pmod m$
/	delen:	c = gehele deel van a / b	$c \equiv a\, b^{-1} \pmod m$
rest	rest bij deling:	c = rest van a / b	
ggd	grootste gemene deler:	$c = \text{ggd}(a,b)$	
wortel	wortel:	c = gehele deel van wortel(a)	

[^]	machtsverheffen:	$c \equiv a^b \pmod m$
[mod m]	reduceren:	als alleen ***a*** ingevuld: $c \equiv a \pmod m$; als ***a*** en ***b*** ingevuld: ***a*** wordt ***a*** (mod ***m***), ***b*** wordt ***b*** (mod ***m***)

De invulvelden ***a***, ***b*** en ***m*** kunt u zelf bewerken zoals in een gewone editor. Het antwoord van een berekening komt in het veld ***c***. In het veld ***c*** kan alleen het programma schrijven.
Als u modulair rekent, moet de modulus ***m*** positief zijn.
Een modulaire inverse kunt u op twee manieren berekenen: als 1 / ***a*** (mod ***m***), en als a^{-1} (mod ***m***).

wis

Klik hierop om alle velden te wissen.

4. Het Kladblok

Het *kladblok* kunt u gebruiken om getallen of teksten tijdelijk in op te slaan. Er zijn tien velden beschikbaar. U kunt er naartoe en vanuit kopiëren op de hier boven beschreven manieren.
De velden kunnen een label hebben (bv. "**p =**"). Daar zijn suggesties ingevuld voor wat u in het veld zou kunnen bewaren. Maar u hoeft zich van die labels niets aan te trekken.
Ook hebben de velden elk een selectievakje. Ze geven aan welke velden weggeschreven dan wel ingelezen worden.
Met de knoppen "publiek", "prive", "bericht", "RSA" en "DH" worden bepaalde velden geselecteerd, volgens onderstaande tabel. Maar u kunt ze ook met de hand aan of uit zetten, naar behoefte.

RSA			DH			bericht		
label	publiek	prive	label	publiek	prive	label	publiek	prive
p		✓	p	✓	✓			
q		✓	g	✓	✓			
n	✓	✓	x		✓			
fi			y	✓	✓			
e	✓	✓	s		✓			
d		✓						
dp		✓						
dq		✓						
B			B			B		✓
G			G			G	✓	✓

Als u DH selecteert verschijnt er ook een keuzelijst "parameters" waarmee u de grootte van ingeprogrammeerde DH-systeemparameters ***p***, ***g*** kunt zetten, die worden dan in de juiste velden klaargezet. U kunt natuurlijk altijd uw eigengekozen DH-systeemparameters gebruiken, als u dat wilt.

In alle velden van het kladblok kunt u ook met de hand editen, kopiëren, knippen en plakken, en met de muis kopiëren.

schrijf weg

Alle gegevens uit de aangevinkte velden in het kladblok worden naar een bestand geschreven.

lees in

Gegevens uit een bestand worden ingelezen in de aangevinkte velden in het kladblok.

wis

Klik hierop om alle velden van het kladblok te wissen.

5. De (Priem)getallenfabriek

Met de *(Priem)getallenfabriek* kunt u willekeurige oneven getallen maken, en ook willekeurige priemgetallen, tot een grootte van 400 cijfers.

Geef het aantal cijfers op dat het te maken getal groot moet zijn, tenminste 1 cijfer, en ten hoogste 400.

maak willekeurig oneven getal

Maak een willekeurig oneven getal. Dit moet razendsnel gaan, ook voor hele grote getallen.

maak willekeurig priemgetal

Maak een willekeurig (oneven) priemgetal. Dit kan enige seconden tot enige minuten duren, zeker voor grote priemgetallen. De rekentijd hangt niet alleen van het aantal opgegeven cijfers en de snelheid van uw computer af, ook voor een vast aantal cijfers en op een vaste computer kan de rekentijd sterk variëren.

zoek volgende priemgetal

Als er een getal in het veld (priem)getal staat, dan wordt dit vervangen door het eerstvolgende priemgetal. Ook dit kan even duren.

wis

Klik hierop om alle velden te wissen.

6. De Tekst-Getal-omzetter

Met de *Tekst-Getal-omzetter* kunt u korte leesbare teksten in getallen omzetten volgens de onderstaande tabel, en omgekeerd getallen in teksten omzetten.

letter	getal	letter	getal	letter	getal	letter	getal	cijfer	getal	symbool	getal
a	10	n	23	A	40	N	53	0	70	(spatie)	80
b	11	o	24	B	41	O	54	1	71	, (komma)	81
c	12	p	25	C	42	P	55	2	72	. (punt)	82
d	13	q	26	D	43	Q	56	3	73	! (uitroepteken)	83
e	14	r	27	E	44	R	57	4	74	? (vraagteken)	84
f	15	s	28	F	45	S	58	5	75	((haakje openen)	85
g	16	t	29	G	46	T	59	6	76	) (haakje sluiten)	86
h	17	u	30	H	47	U	60	7	77	- (min)	87
i	18	v	31	I	48	V	61	8	78	+ (plus)	88
j	19	w	32	J	49	W	62	9	79	= (is)	89
k	20	x	33	K	50	X	63				
l	21	y	34	L	51	Y	64				
m	22	z	35	M	52	Z	65				

Andere tekens zijn niet toegestaan.
Voorbeeld: "Hallo daar!" wordt "4710212124801310102783".

Ook kunt u terug: een getal kunt u weer omzetten naar de tekst. Alle hierboven niet-genoemde combinaties van twee cijfers (00-09, 36-39, 66-69, 90-99) worden teruggezet naar spaties. Van een getal met een oneven aantal cijfers wordt het eerste cijfer genegeerd.

v v v tekst ==> getal v v v

Zet de tekst in het bovenste invulveld om in een getal, dat in het onderste invulveld getoond wordt.

^ ^ ^ getal ==> tekst ^ ^ ^

Zet het getal in het onderste invulveld om in een tekst, die in het bovenste invulveld getoond wordt.

wis

Klik hierop om alle velden te wissen.

Gebruiksvoorbeeld 1 - RSA: sleutelpaar maken

- Selecteer bij het kladblok de optie "RSA".
- Stap 1: maak de modulus:
  - Bedenk hoeveel cijfers de modulus ongeveer moet worden (maximaal 800).
  - Maak m.b.v. de (priem)getallenfabriek een priemgetal ***p*** dat de helft van dat aantal cijfers heeft.
  - Verplaats ***p*** naar het kladblok in het veld voor ***p***, en ook naar het veld ***a*** in de rekenmachine.
  - Maak m.b.v. de (priem)getallenfabriek een tweede priemgetal ***q*** met evenveel cijfers als ***p***.
  - Verplaats ***q*** naar het kladblok in het veld voor ***q***, en ook naar het veld ***b*** in de rekenmachine.
  - Zet de rekenmachine op niet-modulair.
  - Vermenigvuldig ***a*** en ***b***. Dit is de RSA-modulus ***n***, gelijk aan ***p*** maal ***q***.
  - Verplaats ***n*** naar het kladblok in het veld voor ***n***.
- Stap 2: maak ***fi(n)***:
  - Verminder in de rekenmachine met de hand ***a*** en ***b*** met 1 (klik in het veld, en ga met de END-toets naar het laatste cijfer, selecteer dit en vervang het door 1 minder).
  - Vermenigvuldig de nieuwe ***a*** en ***b***. Dit wordt ***fi(n)***, de Euler-***fi***-functie van ***n***, deze is gelijk aan ***p-1*** maal ***q-1***. Let erop dat ongeveer de eerste helft van de cijfers van ***fi (n)*** en ***n*** identiek zijn, maar de laatste helft verschillend.
  - Verplaats ***fi(n)*** naar het kladblok in het veld voor ***fi***.
- Stap 3: maak de publieke exponent:
  - Maak m.b.v. de (priem)getallenfabriek een oneven getal ***e*** van tenminste één minder dan het aantal cijfers van ***n***. Dit is de publieke exponent.
  - Verplaats ***e*** naar het kladblok in het veld voor ***e***.
- Stap 4: maak de privé-exponent:
  - Verplaats ***fi*** naar het veld ***b*** in de rekenmachine, en ***e*** naar het veld ***a***.
  - Bereken ggd(***a***,***b***), m.a.w. ggd(***e***,***fi***). Als deze niet gelijk is aan 1, begin dan overnieuw met Stap 3, net zo lang tot in dit stadium wel ggd(***e***,***fi***) = 1. Tip: kies voor ***e*** in Stap 3 een priemgetal, dat verhoogt de kans op een ggd van 1 aanzienlijk.
  - Zet de rekenmachine op modulair.
  - Verplaats in de rekenmachine ***fi*** (die staat nog steeds in het veld ***b***) naar het veld ***m***.
  - Zet -1 in het veld ***b*** in de rekenmachine.
  - Verhef ***a*** tot de macht ***b*** (mod ***m***), m.a.w. bereken $\boldsymbol{d} = \boldsymbol{e}^{-1}$ (mod ***fi***). Dit wordt de privé-exponent.
  - Verplaats ***d*** naar het kladblok in het veld voor ***d***.
- Stap 5: sla het sleutelpaar op in twee bestanden:
  - Selecteer de optie "prive". Klik op "schrijf weg", om de getallen ***n***, ***e*** en ***d*** in een bestand (standaard met extensie .txt) op te slaan. Dit bestand moet u zien als uw privésleutel-bestand. Geef het een toepasselijke naam (bv. mijnprivesleutel.txt), en plaats het in een handige map. Dit bestand moet u niet uit handen geven.
  - Selecteer de optie "publiek". Klik nogmaals op "schrijf weg", om de getallen ***n*** en ***e*** in een tweede bestand (weer standaard met extensie .txt) op te slaan. Dit bestand moet u zien als uw publieke-sleutel-bestand. Geef het een toepasselijke naam (bv. mijnpubliekesleutel.txt), en plaats het in een handige map. Dit bestand kunt u aan anderen geven.

Gebruiksvoorbeeld 2 - RSA: versleutelen

Dit kunt u doen met een publieke sleutel (***n*** en ***e***) die u van iemand anders hebt gekregen, en aan wie u een geheim wilt versturen.

- Selecteer bij het kladblok de opties "RSA" en "publiek".

- Lees de publieke sleutel uit een bestand, via de knop "lees in" bij het kladblok.
- Zet de rekenmachine op modulair.
- Verplaats de modulus ***n*** naar het veld ***m*** in de rekenmachine.
- Verplaats de publieke exponent ***e*** naar het veld ***b*** in de rekenmachine.
- Zet de te versleutelen tekst in het tekst-veld in de tekst-getal omzetter.
- Zet de te versleutelen tekst om in een getal, ***B***. Zorg er voor dat ***B*** kleiner is dan de modulus ***n***, anders gaat het straks fout (U kunt de te versleutelen tekst desgewenst in stukken opdelen, en alle stukken apart te behandelen). Verplaats dit getal naar het kladblok in het veld voor ***B***.
- Verplaats ***B*** naar het veld ***a*** in de rekenmachine.
- Verhef ***a*** tot de macht ***b*** (mod ***m***).
- Het getal in het veld ***c*** is nu het geheimschrift ***G***. Verplaats dit naar het kladblok in het veld voor ***G***.
- Als u ***B*** in een bestand wilt opslaan, selecteer dan de opties "bericht" en "prive", en schrijf weg. Het bestand met ***B*** erin moet u niet publiek maken of over een onveilig kanaal versturen, want ***B*** is onversleuteld.
- Als u ***G*** in een bestand wilt opslaan, selecteer dan de opties "bericht" en "publiek", en schrijf weg. Het bestand met ***G*** erin mag u gerust publiek maken en over een onveilig kanaal versturen, want ***G*** is versleuteld.

Gebruiksvoorbeeld 3 - RSA: ontsleutelen

Dit kunt u doen met uw eigen privésleutel (***n*** en ***d***), en met een geheimschrift dat door iemand anders met uw publieke sleutel versleuteld is.

- Selecteer bij het kladblok de opties "RSA" en "prive".
- Lees de privésleutel uit een bestand, via de knop "lees in" bij het kladblok.
- Zet de rekenmachine op modulair.
- Verplaats de modulus ***n*** naar het veld ***m*** in de rekenmachine.
- Verplaats de privé-exponent ***d*** naar het veld ***b*** in de rekenmachine.
- Selecteer bij het kladblok de opties "bericht" en "publiek".
- Lees het geheimschrift in uit een bestand, via de knop "lees in" bij het kladblok. Het komt in het veld voor ***G*** te staan.
- Zet ***G*** in het veld ***a*** in de rekenmachine.
- Verhef ***a*** tot de macht ***b*** (mod ***m***).
- Het getal in het veld ***c*** is nu het oorspronkelijke bericht ***B***. Verplaats ***B*** naar het veld voor ***B*** in het kladblok.
- Verplaats ***B*** naar het veld voor het getal in de tekst-getal omzetter.
- Zet het getal om in tekst. Als alles goed is gegaan verschijnt de oorspronkelijke tekst, en heeft u het geheim leesbaar gemaakt.

Gebruiksvoorbeeld 4 - RSA: handtekening maken

Dit kunt u doen met uw eigen privésleutel (in de vorm ***n*** en ***d***), en met iedere tekst (die niet versleuteld is, anders weet u niet wat u tekent).

- Selecteer bij het kladblok de opties "RSA" en "prive".
- Lees de privésleutel in uit een bestand, via de knop "lees in" bij het kladblok.
- Zet de rekenmachine op modulair.
- Verplaats de modulus ***n*** naar het veld ***m*** in de rekenmachine.
- Verplaats de privé-exponent ***d*** naar het veld ***b*** in de rekenmachine.
- Zet de te ondertekenen tekst in het tekst-veld in de tekst-getal omzetter.
- Zet de te ondertekenen tekst om in een getal, ***B***. Zorg er voor dat ***B*** kleiner is dan de modulus ***n***, anders gaat het straks fout (U kunt de te versleutelen tekst desgewenst in stukken opdelen, en alle stukken apart te behandelen). Verplaats dit getal naar het kladblok in het veld voor ***B***. Let wel: het getal ***B*** is in dit geval niet geheim.
- Verplaats ***B*** naar het veld ***a*** in de rekenmachine.
- Verhef ***a*** tot de macht ***b*** (mod ***m***).

- Het getal in het veld ***c*** is nu uw handtekening die hoort bij uw tekst. U kunt de handtekening desgewenst in een bestand oposlaan.

Gebruiksvoorbeeld 5 - RSA: handtekening controleren

Dit kunt u doen met een publieke sleutel (***n*** en ***e***) die u van iemand anders hebt gekregen, en van wie u een tekst met bijbehorende handtekening hebt gekregen.

- Selecteer bij het kladblok de opties "RSA" en "prive".
- Lees de publieke sleutel uit een bestand, via de knop "lees in" bij het kladblok.
- Zet de rekenmachine op modulair.
- Verplaats de modulus ***n*** naar het veld ***m*** in de rekenmachine.
- Verplaats de publieke exponent ***e*** naar het veld ***b*** in de rekenmachine.
- Zet de handtekening in het veld ***a*** in de rekenmachine. Wellicht kon u de handtekening uit een bestand inlezen.
- Verhef ***a*** tot de macht ***b*** (mod ***m***).
- Zet de ondertekende tekst in het tekst-veld in de tekst-getal omzetter.
- Zet de ondertekende tekst om in een getal. Dit getal moet nu precies gelijk zijn aan het getal ***c*** in de rekenmachine. Als dat inderdaad zo is, dat weet u zeker dat de eigenaar van deze publieke sleutel deze tekst heeft ondertekend. Als de twee getallen niet hetzelfde zijn, is er ergens iets fout gegaan. Als u zeker bent dat u niets fout hebt gedaan, dan betekent dat dat de handtekening niet klopt, en dat ofwel de tekst niet origineel is, ofwel de ondertekenaar iemand anders is dan hij voorgeeft te zijn.

Gebruiksvoorbeeld 6 - Diffie-Hellman: gedeeld geheim afspreken

Personen ***A*** en ***B*** willen een gezamenlijk geheim getal afspreken, bijvoorbeeld om daar een wachtwoord uit af te leiden. Maar het communicatiekanaal dat ze gebruiken is af te luisteren. Hoe kunnen ze dit oplossen?

Niet helemaal realistisch, voeren we in dit voorbeeld alle berekeningen uit in hetzelfde programma.

- Selecteer bij het kladblok de optie "DH".
- Stap 1: maak systeemparameters:
  - U kunt voorgeprogrammeerde systeemparameters gebruiken, als u dat wilt selecteert u in de keuzelijst "parameters" een lengte, de parameters ***p***, ***g*** verschijnen dan in het kladblok. Als u daarmee tevreden bent kunt u meteen door met stap 2. Als u eigen systeemparameters wilt maken, maakt u stap 1 verder af.
  - Bedenk hoeveel cijfers u wilt voor de modulus ***p***, maximaal 400.
  - Maak met behulp van de "(priem)getallenfabriek" een priemgetal ***p***, en verplaats dit naar de juiste plaats in het kladblok. Dit getal wordt de modulus voor Diffie-Hellman.
  - Maak met behulp van de "(priem)getallenfabriek" een oneven getal ***g***, met het aantal cijfers één minder dan dat van ***p***, en verplaats dit naar de juiste plaats in het kladblok.
- Stap 2: persoon ***A*** maakt een sleutelpaar:
  - Maak met behulp van de "(priem)getallenfabriek" een oneven getal ***x*** met een aantal cijfers dat één minder is dan dat van ***p***, en verplaats dit naar de juiste plaats in het kladblok. Dit getal ***x*** is de privésleutel van ***A***.
  - Verplaats ***p*** van het kladblok naar het veld voor de modulus ***m*** in de rekenmachine.
  - Verplaats ***g*** van het kladblok naar het veld voor ***a*** in de rekenmachine.
  - Verplaats ***x*** van het kladblok naar het veld voor ***b*** in de rekenmachine.
  - Bereken $y = g^x \pmod{p}$. Dit getal ***y*** is de publieke sleutel van ***A***.
  - Verplaats ***y*** van het veld voor ***c*** in de rekenmachine naar de juiste plaats in het kladblok.
- Stap 3: persoon ***B*** maakt een sleutelpaar:

    - Maak met behulp van de "(priem)getallenfabriek" een oneven getal x' met een aantal cijfers dat één minder is dan dat van p, en verplaats dit naar de juiste plaats in het kladblok. Dit getal x' is de privésleutel van ***B***.
    - Verplaats p van het kladblok naar het veld voor de modulus m in de rekenmachine.
    - Verplaats g van het kladblok naar het veld voor a in de rekenmachine.
    - Verplaats x' van het kladblok naar het veld voor b in de rekenmachine.
    - Bereken $y' = g^{x'} \pmod{p}$. Dit getal y' is de publieke sleutel van ***B***.
    - Verplaats y' van het veld voor c in de rekenmachine naar de juiste plaats in het kladblok.
- Stap 4: persoon ***A*** maakt het gezamenlijke geheim:
    - Wis alle getallen in de rekenmachine.
    - Verplaats p van het kladblok naar het veld voor de modulus m in de rekenmachine.
    - Verplaats y' van het kladblok naar het veld voor a in de rekenmachine.
    - Verplaats x van het kladblok naar het veld voor b in de rekenmachine.
    - Bereken $s = y'^{x} \pmod{p}$. Dit getal s is het gezamenlijke geheim, berekend door ***A***.
    - Verplaats s van het veld voor c in de rekenmachine naar de juiste plaats in het kladblok.
- Stap 5: persoon ***B*** maakt het gezamenlijke geheim:
    - Wis alle getallen in de rekenmachine.
    - Verplaats p van het kladblok naar het veld voor de modulus m in de rekenmachine.
    - Verplaats y van het kladblok naar het veld voor a in de rekenmachine.
    - Verplaats x' van het kladblok naar het veld voor b in de rekenmachine.
    - Bereken $s' = y^{x'} \pmod{p}$. Dit getal s' is het gezamenlijke geheim, berekend door ***B***.
    - Verplaats s' van het veld voor c in de rekenmachine naar de juiste plaats in het kladblok.
- Controleer in het kladblok dat beide personen hetzelfde geheime getal hebben gemaakt, m.a.w. dat $s = s'$.

Let erop dat elk van de personen ***A*** en ***B*** alleen zijn eigen privésleutel heeft gebruikt, en van de andere persoon alleen de publieke sleutel hoeft te weten.
Via het kladblok zijn de verschillende getallen desgewenst naar bestanden weg te schrijven.

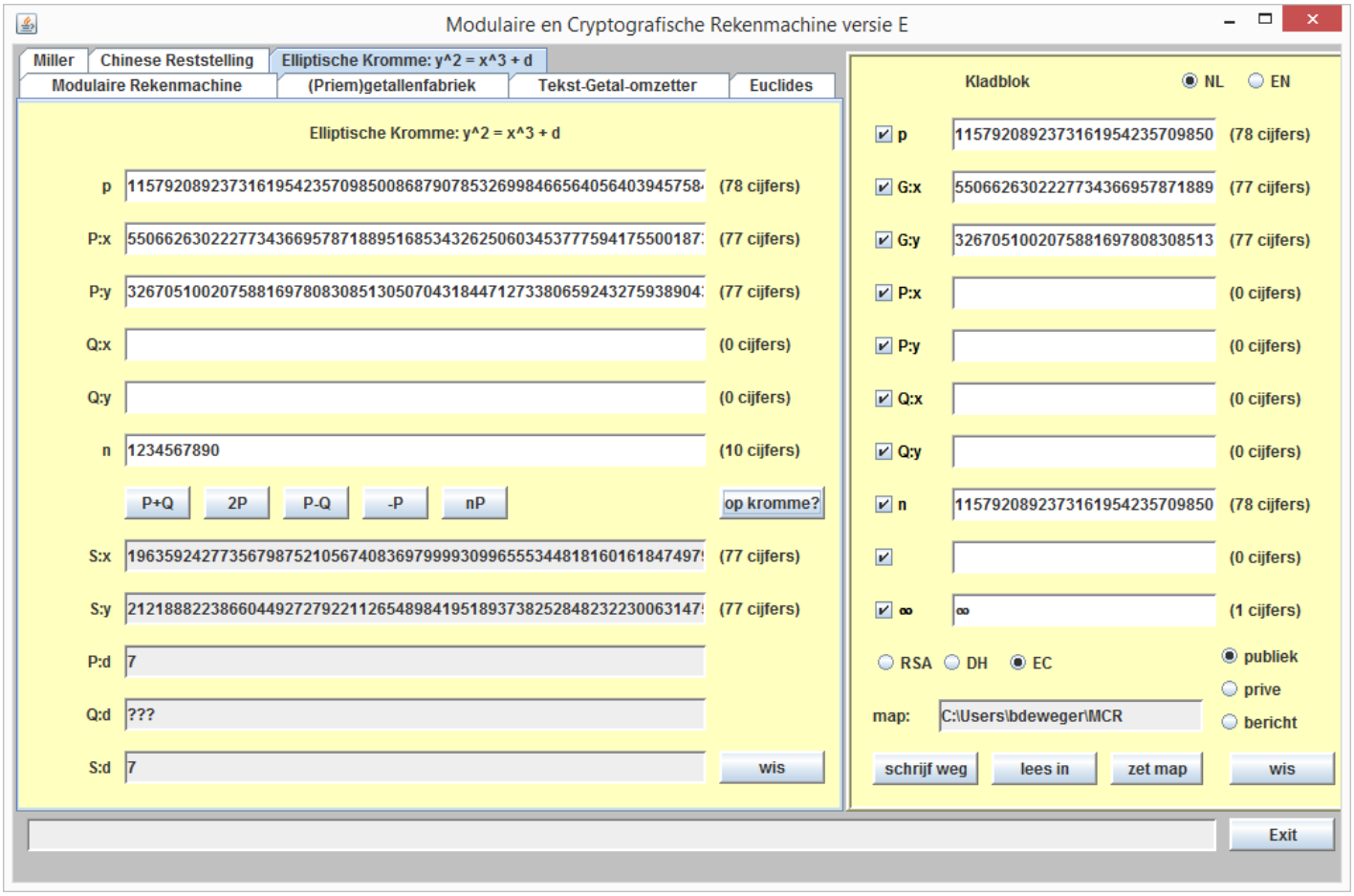
Een realistischer variant van Diffie-Hellman

Het is realistischer om de acties van personen ***A*** en ***B*** op verschillende computers uit te voeren, door verschillende personen, en met een afluisteraar ***E*** die alle communicatie tussen ***A*** en ***B*** kan inzien (maar niet kan wijzigen). Dat kan als volgt.

- ***A*** doet eerst stap 1 en 2, en schrijft de berekende getallen naar twee bestanden: één met zijn privésleutel (de getallen p, g, x en y naar A-pri.txt) en één met zijn publieke sleutel (de getallen p, g en y naar A-pub.txt).
- ***A*** stuurt het bestand A-pub.txt naar ***B***.
- ***E*** onderschept het bestand A-pub.txt, en komt zo p, g en y te weten. Het bestand moet wel ongewijzigd bij ***B*** aankomen.
- ***B*** leest het bestand A-pub.txt in. Let op: in het veld voor y komt dan de publieke sleutel van A te staan. Het is handig deze naar het veld voor y' te verplaatsen. Nu doet B stap 3. Hij schrijft de berekende getallen naar twee bestanden: één met zijn privésleutel (de getallen p, g, x en y naar B-pri.txt) en één met zijn publieke sleutel (de getallen p, g en y naar B-pub.txt)..
- ***B*** stuurt het bestand B-pub.txt naar ***A***.
- ***B*** kan nu ook alvast stap 5 doen om het gedeelde geheime getal te berekenen.
- ***E*** onderschept het bestand B-pub.txt, en komt zo, naast p, g en de y van A, ook nog de y van B te weten. Het bestand moet wel ongewijzigd bij ***A*** aankomen.

- ***A*** leest het bestand B-pub.txt in. Maar let op: in het veld voor ***y*** komt dan de publieke sleutel van B te staan. Het is handig deze naar het veld voor ***y'*** te verplaatsen. A heeft haar eigen publieke sleutel op dit moment niet nodig. Nu doet A stap 4 om het gedeelde geheime getal te berekenen.
- ***A*** en ***B*** hebben nu een gedeeld geheim getal. Afluisteraar ***E***, die de communicatie tussen ***A*** en ***B*** helemaal heeft afgeluisterd, kan toch het geheime getal van ***A*** en ***B*** niet berekenen.
- Om deze sleutels te gebruiken kan bijvoorbeeld een heel eenvoudige manier van versleutelen en ontsleutelen gebruikt worden:
  versleutelen: $G = B \times s \pmod{p}$,
  ontsleutelen: $B = G / s \pmod{p}$,

MCRE Elliptische Krommen Rekenmachine – Handleiding



Om het programma te starten, dubbelklik het MCRE-icoon, of voer "java -jar MCRE.jar" in op een commando-regel.

Zet (in de rechter bovenhoek) de taal op NL (of niet).

Op het kladblok, bijna onderaan, zie je knoppen RSA, DH, EC; kies EC.

Dan zie je in het kladblok de parameters van de Bitcoin-kromme verschijnen: het priemgetal p, de coördinaten G:x, G:y, van de voortbrenger G, en de orde n (het lijkt alsof n = p maar dat is alleen waar voor de bovenste helft van de cijfers).

Alle getallen worden weergegeven in decimale notatie.

Sleep getallen met je muis van het ene veld naar het andere. Ook CTRL-C, CTRL-V werken zoals je denkt. Let op: als je met je muis een x- of y-coördinaat van een punt op de kromme versleept, dan gaat de andere coördinaat ook mee.

Om het punt op oneindig weer te geven, gebruik je het symbool ∞ voor beide coördinaten. Je kunt het symbool ∞ invoeren door te slepen uit het kladblok, waarin het onderaan voor je klaarstaat, maar (in ieder geval op een Windows-systeem) kun je het ook intypen als ALT-236, dat wil zeggen, door de ALT-toets ingedrukt te houden terwijl je 236 intoetst op het numerieke deel van je toetsenbord.

Namen van de velden in het kladblok zijn alleen maar suggesties, je kunt die velden gebruiken voor wat je maar wilt.

Voer een priemgetal p in, en punten P = (P:x,P:y), Q = (Q:x,Q:y) (voor het punt op oneindig: (∞,∞)). Dan kun je de volgende operaties uitvoeren (in alle 5 gevallen verschijnt het antwoord als punt S = (S:x,S:y)):

- P+Q : optelling van P en Q
- 2P : verdubbeling van P
- P-Q: aftrekken van Q van P af
- -P : tegengestelde van P
- nP : vermenigvuldig het punt P met het getal n

De knop "op kromme?" berekent voor de punten P, Q en S de waarde van d = y^2 - x^3 (mod p). Die moeten gelijk (or ∞) zijn, willen de operaties enige zin hebben. Voor de BitCoin-kromme is altijd d = 7.

Disclaimer

De MCRE-software is uitsluitend bedoeld voor educatieve doeleinden, is niet geschikt voor ander dan educatief gebruik, en voldoet aan geen enkele beveiligingsstandaard.

Er wordt geen ondersteuning of goed functioneren gegarandeerd. Gebruik is geheel voor eigen risico.
Suggesties voor verbetering zijn uiteraard van harte welkom.
De software is getest met Java 1.8 op Windows.

versie E.1: 2018