1. Testen ElGamal

Im Vorgriff auf die Checkliste habe ich mir mal ElGamal angesehen. Leider fiel mir noch viel auf:

a) Beim Ändern der Fenstergröße kommen die Scrollbars (vertikal und horizontal) korrekt.

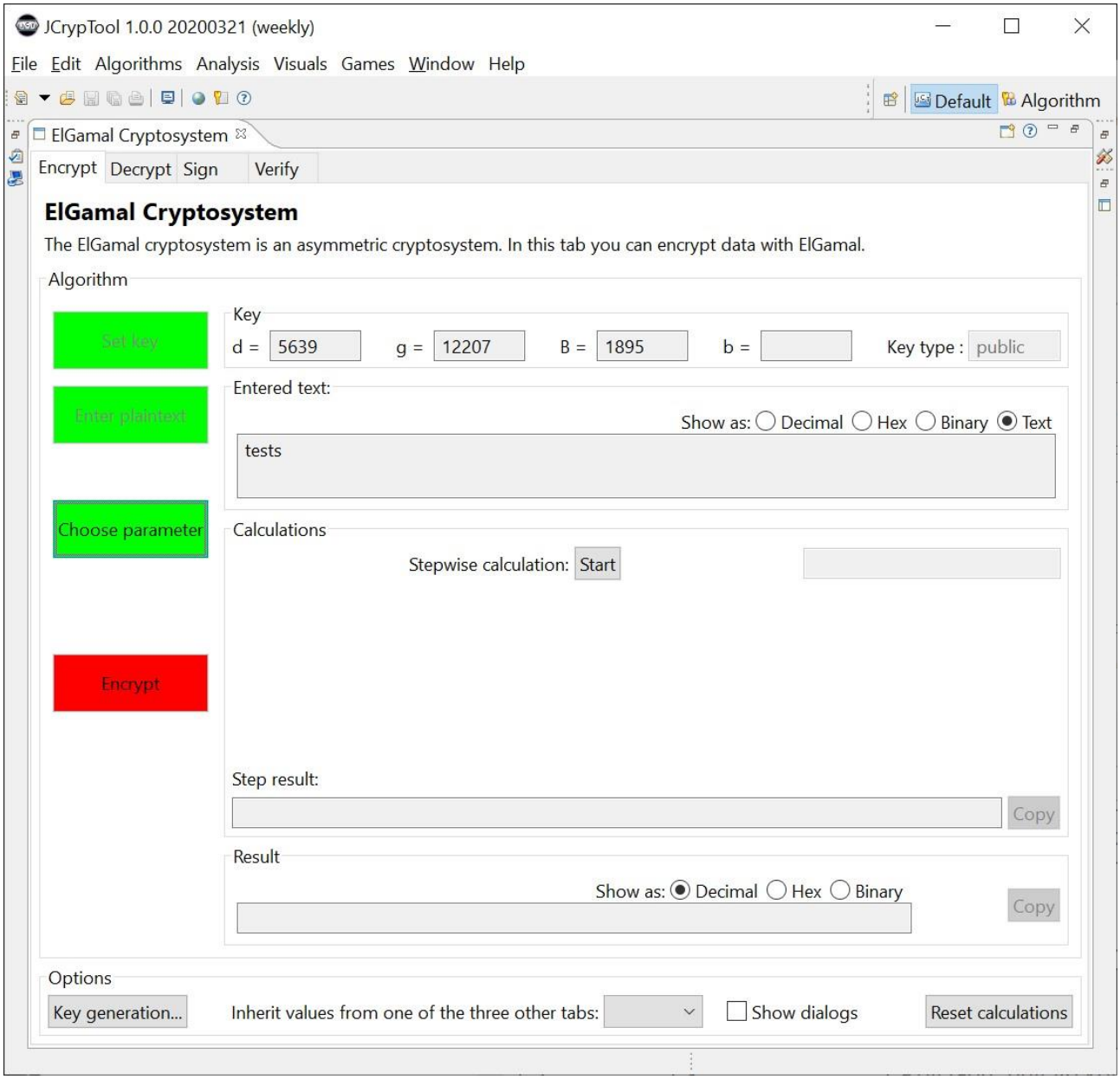
b) Bei asymmetrischen Verfahren ist es besser, man gibt an, wer an wen verschlüsselt Nachrichten schickt. Bitte Beschreibungstext ändern:

E: The ElGamal cryptosystem is an asymmetric cryptosystem. In this tab you can encrypt data with ElGamal.
==>
The ElGamal cryptosystem is an asymmetric encryption and signing system. In this tab Alice encrypts data with ElGamal for Bob.

D: In diesem Tab können Sie Daten mit ElGamal verschlüsseln.
==>
In diesem Tab verschlüsselt Alice Daten mit ElGamal für Bob.

c) yyy

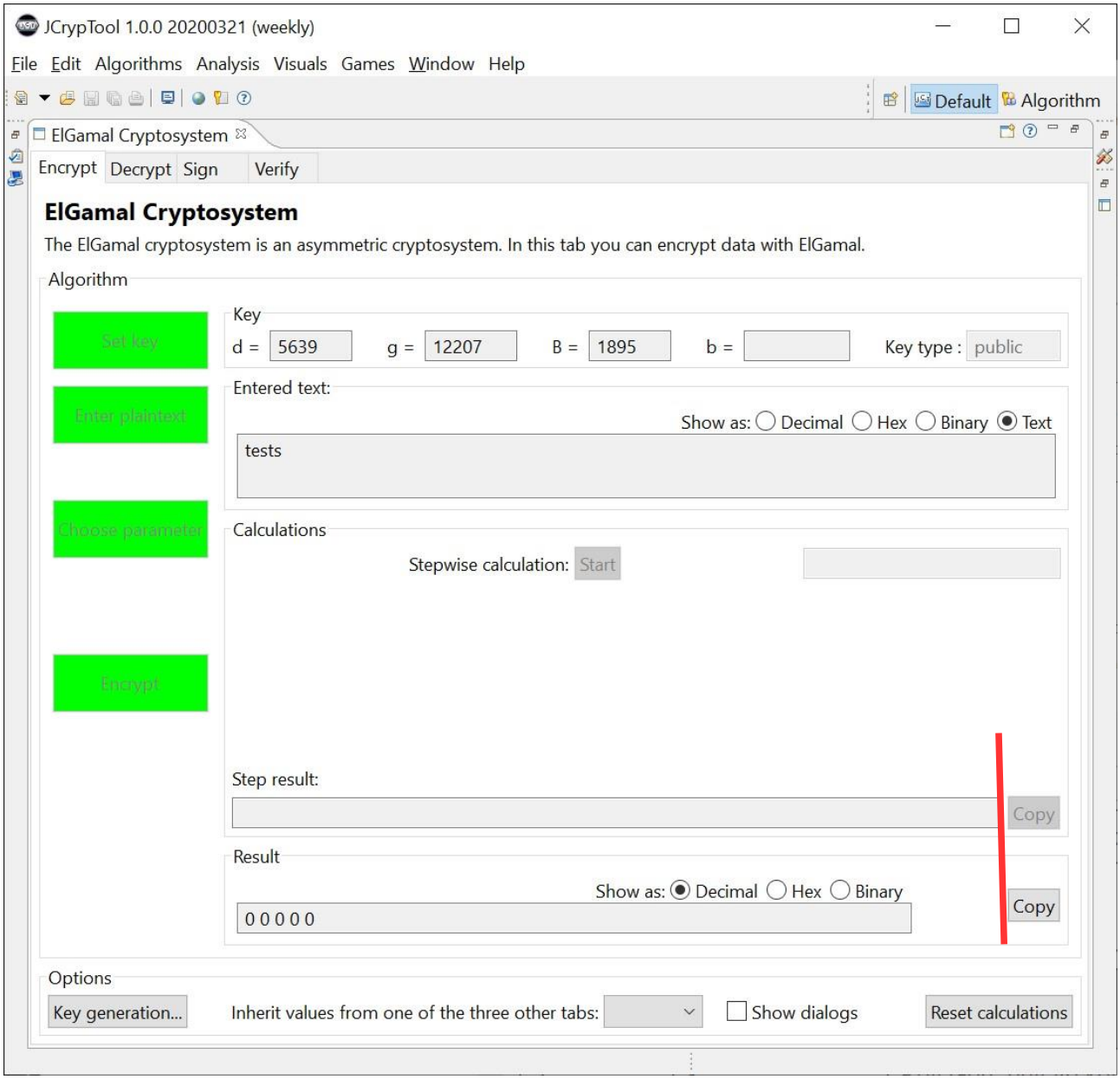
b) Die Choose- und Encrypt-Button stehen irgendwo in der Vertikalen.
d) Der Paramter k wird nicht angezeigt im Fenster (k = number randomly generated per message = secret session key.



--> Wir sollten das Fenster umbauen:
- Den Button "Choose parameter" oberhalb von "Enter plaintext".
- Hinter den Button "Choose parameter" eine Gruppierung "Parameter randomly generated per message = secret session key", die den Wert für k anzeigt.
- Dann kann man den Button "Encrypt" oben bündig mit der Gruppierung "Calculations" setzen.

e) Bisher konnte man nach "Choose parameter" entweder auf "Start" (hinter stepwise calculations") klicken (dann wurden die Ergebnisse pro Zeichen berechnet und unten eingetragen und wenn alle eingetragen waren, wurde der Encrypt-Button automatisch grün) – oder man klickte auf den Button Encrypt und erhielt gleich das Geamtergebnis.

Aber auch wenn ich erst auf Encrypt ging, möchte ich per "Start" die stepwise calculations durchführen können. Die sollten dann an Result nichts mehr ändern, aber die Werte in "Step result" eintragen.



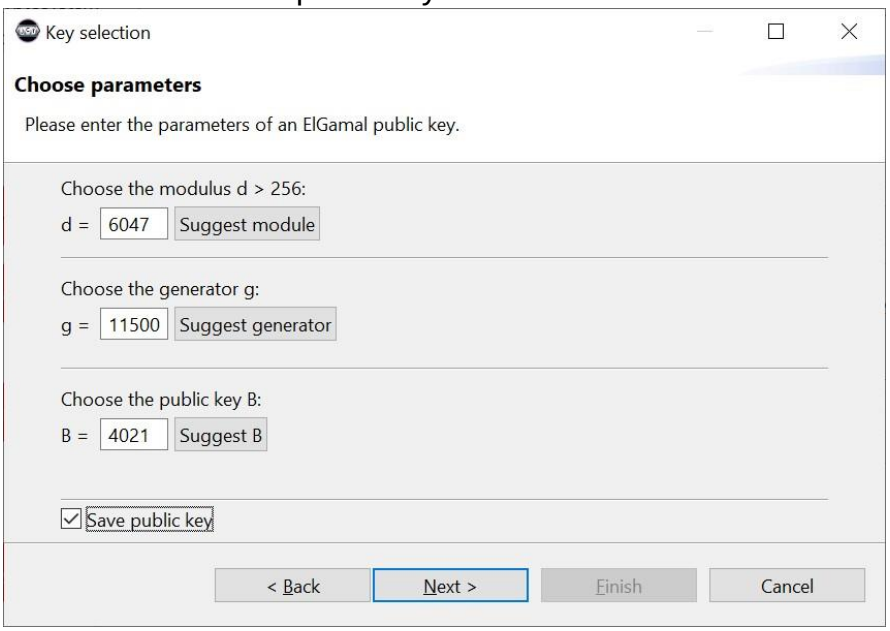
f) Die beiden Ausgabefeld sollten gleich lang sein. Siehe vertikaler roter Strich.

g) ERROR: Das Ergebnis wird falsch berechnet: Ich erhalte momentan immer 0.
h) Nach Klick auf Restart (Neustart) kann ich den Button "Set key" erneut drücken.

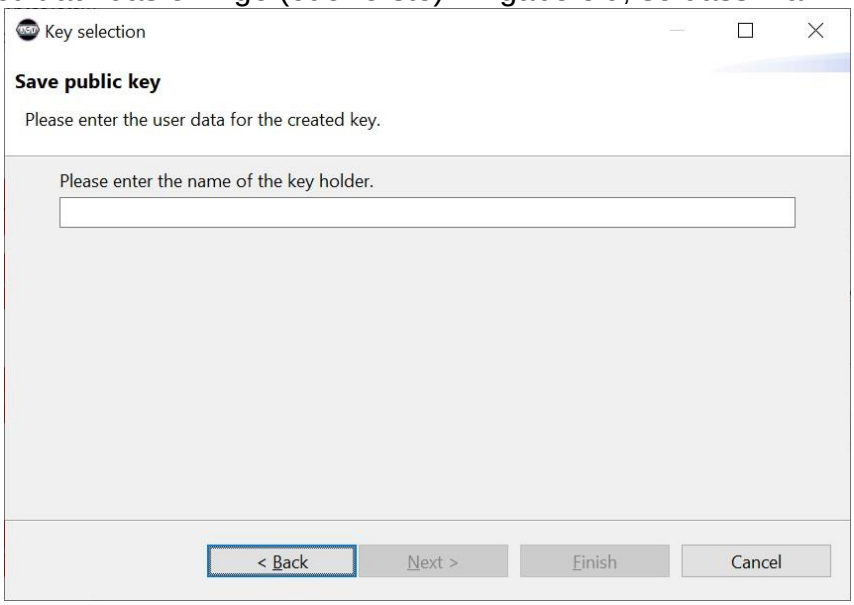
Der Dialog "Key selection" ist mir zu generisch. Bitte den Titel ändern in:
"Key selection for the recipient (usualy Bob)"

i) Optional: Im Folgedialog (Create a new PK) "Key selection"
gleich für d, g und B einen Defaultwert einstellen. Den Button dahinter "Suggest ..." dann ändern in "Suggest another ..."

j) Klickt man oben nach den 3 suggests nicht gleich auf Finish, sondern setzt vorher noch den Haken bei "Save public key"

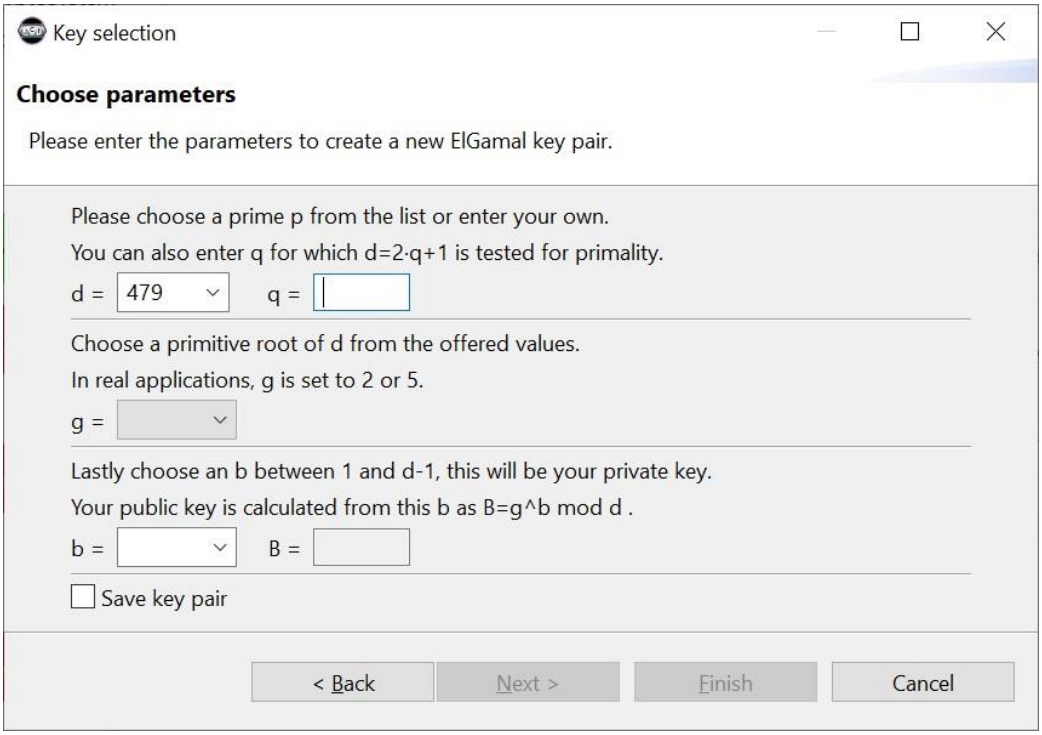


und klickt dann auf Next, kommt der ff. Dialog hoch, aber der Eingabefokus ist nicht gesetzt auf das einzige (oder erste) Eingabefeld, so dass man nicht gleich lostippen kann:



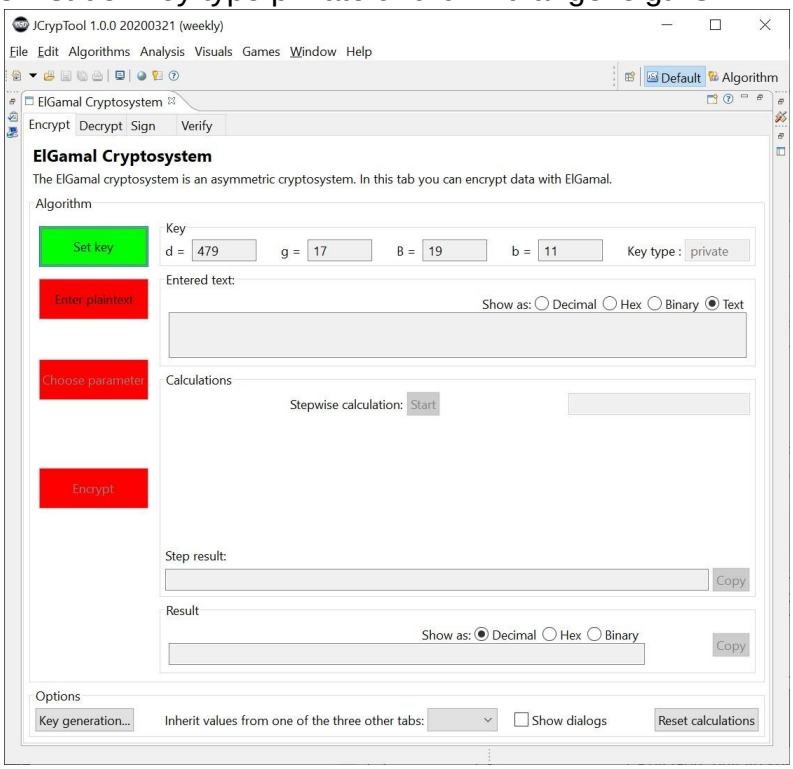
k) Wählt man "Create new public key"bleibt b leer -- weil nur public key erzeugt. --> Vielleicht Balloontext zu b (no privat key of recipient known).

l) Wählt man statt Create new public key den Radiobutton Create new key pair, kommt:



Hier sollten q und B auch einen "Suggest"-Button haben (zusätzlich zur Möglichkeit, die Zahl selbst einzugeben).

Nach Finish ist der Key type private und b wird angezeigt: Ok.



m)"Reset calculations" sollte einen Tooltip haben, dass es auch den eingegebenen Text zurücksetzt.

Und: Es sollte nicht den Parameter k zurücksetzen

n) "Copy" in der Gruppierung "Result" hat bei mir nicht getan.