Christel Bach cb@vibkat.dk 13.dec 2017

Anvendelse af værktøj

Shamir Secret Sharing med Lagrange polynomier

http://christelbach.com
Shamir Secret Sharing værktøj findes nederst på siden

Polynomier af første grad

Fuld version
Med værktøjet kan følgende beregnes

- Nøglegenerering (2 punkter) på baggrund af valg af hemmelighed der ønskes delt.
- generering af tilfældige tal (koefficienterne og nøgle del 1) op til ønsket maksimal størrelse.
- hemmeligheden kan beregnes på baggrund af to nøgler
- Lagrange polynomier beregnes på baggrund af to nøgler
- Funktion på baggrund af lagrange polynomier

Vejleding:

Nøglegenerering

1. Vælg maksimal værdi for tilfældigt genererede tal, indtast n. Den står som udgangspunkt til værdien 10
2. Udfyld den ønskede hemmelighed: værdien a0
3. Generer tilfældigt a1, x1, og x2 (kan også udfyldes med ønskede værdier)
4. Tryk på beregn nøgler.
   (Alle ovenstående felter skal være udfyldt for at det virker)
5. Ønskes flere nøgler kan nye værdier af x1 og x2 blot indtastes og nøgler genereres.

Bemærk: For nemheds skyld er værdierne i *denne version* overført værdierne til felterne nederst. De kan blot slettes om ønsket. De to sektioner virker uafhængigt af hinanden.

Afsløring af hemmelighed

1. Indtast to nøgler (to punkter)
   (alle fire felter skal udfyldes)
2. Tryk ”afslør”

   Følgende bliver beregnet
   De to ligninger med to ubekendte der skal løses
   Koefficienterne
   Pointering af hvilken koefficient der er hemmeligheden
   Lagrange polynomierne
   Funktionen på baggrund af lagrange polynomiet
   (både et delresultat og den endelig funktion)

Christel Bach cb@vibkat.dk 13.dec 2017

Polynomier af anden grad

Fuld version
Med værktøjet kan følgende beregnes

- Nøglegenerering (3 punkter) på baggrund af valg af hemmelighed der ønskes delt.
- generering af tilfældige tal (koefficienterne og nøgle del 1) op til ønsket maksimal størrelse.
- hemmeligheden kan beregnes på baggrund af tre nøgler
- Lagrange polynomier beregnes på baggrund af tre nøgler
- Funktion på baggrund af lagrange polynomier

Vejleding:

Nøglegenerering

6. Optionelt: vælg maksimal værdi for tilfældigt genererede tal, indtast n. Den står som udgangspunkt til værdien 10
7. Udfyld den ønskede hemmelighed: værdien a0
8. Generer tilfældigt a1, og a2. x1, x2 og x3 udfyldes med forskellige ønskede værdier.
(Bemærk: i denne version tjekkes IKKE for om x1,x2 og x3 er forskellige)
9. Tryk på beregn nøgler.
(Alle ovenstående felter skal være udfyldt for at det virker)
10. Ønskes flere nøgler kan nye værdier af x1, x2, og x3 blot indtastes og nøgler genereres.

De to hovedsektioner virker uafhængigt af hinanden.

Afsløring af hemmelighed

3. Indtast tre nøgler (tre punkter)
(alle seks felter skal udfyldes)
4. Tryk ”afslør”

Følgende bliver beregnet
Koefficienterne
(de tre ligninger med tre ubekendte skrives IKKE i denne version (kommer evt))
Pointering af hvilken koefficient der er hemmeligheden
Lagrange polynomierne
Funktionen på baggrund af lagrange polynomiet
(både et delresultat og den endelig funktion)
I denne version kan der forekomme små afrundingsfejl

Christel Bach cb@vibkat.dk 13.dec 2017

Polynomier af første grad - elevversion

Elev version
Med værktøjet kan følgende udføres

- Nøglegenerering (2 punkter) på baggrund af valg af hemmelighed der ønskes delt.
- generering af tilfældige tal (koefficienterne og nøgle del 1) op til ønsket maksimal størrelse.. Nøglernes 2. del vises ikke.
- Eleven indtaster nøglernes 2. Del og systemet tjekker om det indtastede er korrekt
- Afsløring af hemmelighed på baggrund af to indtastede punkter. Hemmeligheden vises ikke
- Eleven indtaster hvad hemmeligheden er efter deres beregning og systemet tjekker om svaret er korrekt.

Om værktøjet:
Planlagte udvidelser:
Elev tjek af beregning af Lagrange polynimoer
Elev version af 2. Grad.
Valg af ønsket antal lodder

Værktøjet er programmeret i Javascript og JQuery. Alle beregninger foretages på klienten.
Værktøjet er udviklet som tilbehør til et undervisningsforløb i Shamir Secret Sharing og Lagrange Polynomier. Undervisningsforløbet er udviklet af Clemens Nordentoftm Gert Hedegaard og Jonatan Fredgaard, Viborg Gymnasium og HF, Værktøjet er udviklet af Christel Bach Viborg Katedralskole.
Undervisningsforløbet kan findes her

/CB