Beveilig je data met priemgetallen



WEETJE
Wist je dat de Griekse wiskundige Euclides zich rond 300 voor Christus al bezig hield met priemgetallen?

Als je een bericht stuurt naar iemand via bijvoorbeeld WhatsApp of Telegram dan is dat bedoeld voor die persoon. Het is niet fijn als andere mensen mee kunnen lezen. Daarom zijn al deze berichten versleuteld met een beveiligingssleutel. Deze sleutel bestaat uit het product van twee priemgetallen. In deze lesbrief gaan jullie je eigen beveiligingssleutel maken. Let op: zorg dat het een goede sleutel is, want later gaan jullie klasgenoten deze proberen te kraken!

OPDRACHT 1 – Zoek de priemgetallen

Om een sleutel te kunnen maken, heb je twee grote priemgetallen nodig. Om die te vinden kun je de zeef van Eratosthenes gebruiken. Bekijk deze video tot 0:53.

Streep in de zeef van Eratosthenes op de volgende pagina alle getallen weg die geen priemgetal zijn.

Stichting FutureNL ontwikkelt onafhankelijk lesmateriaal. © 2022 Iedereen mag deze les downloaden, delen en uitprinten (alleen niet als je er geld mee wilt verdienen). Doen! Creative Commons licence: CC BY-NC-ND 4.0. Deze les is gemaakt door Sjoukje Wisman en Karlijn Ballemans van WisMon.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100
101	102	103	104	105	106	107	108	109	110
111	112	113	114	115	116	117	118	119	120
121	122	123	124	125	126	127	128	129	130
131	132	133	134	135	136	137	138	139	140
141	142	143	144	145	146	147	148	149	150

Schrijf de priemgetallen hieronder naast elkaar op:

OPDRACHT 2 – Maak een beveiligingssleutel

Kies nu twee priemgetallen uit het lijstje dat je bij opdracht 1 hebt opgesteld. Let op: hoe groter de priemgetallen, hoe moeilijker de sleutel te kraken is.

Wij kiezen de volgende twee priemgetallen:

Vermenigvuldig de twee priemgetallen met elkaar. Je krijgt zo jullie beveiligingssleutel.

Onze beveiligingssleutel is:

WEETJE

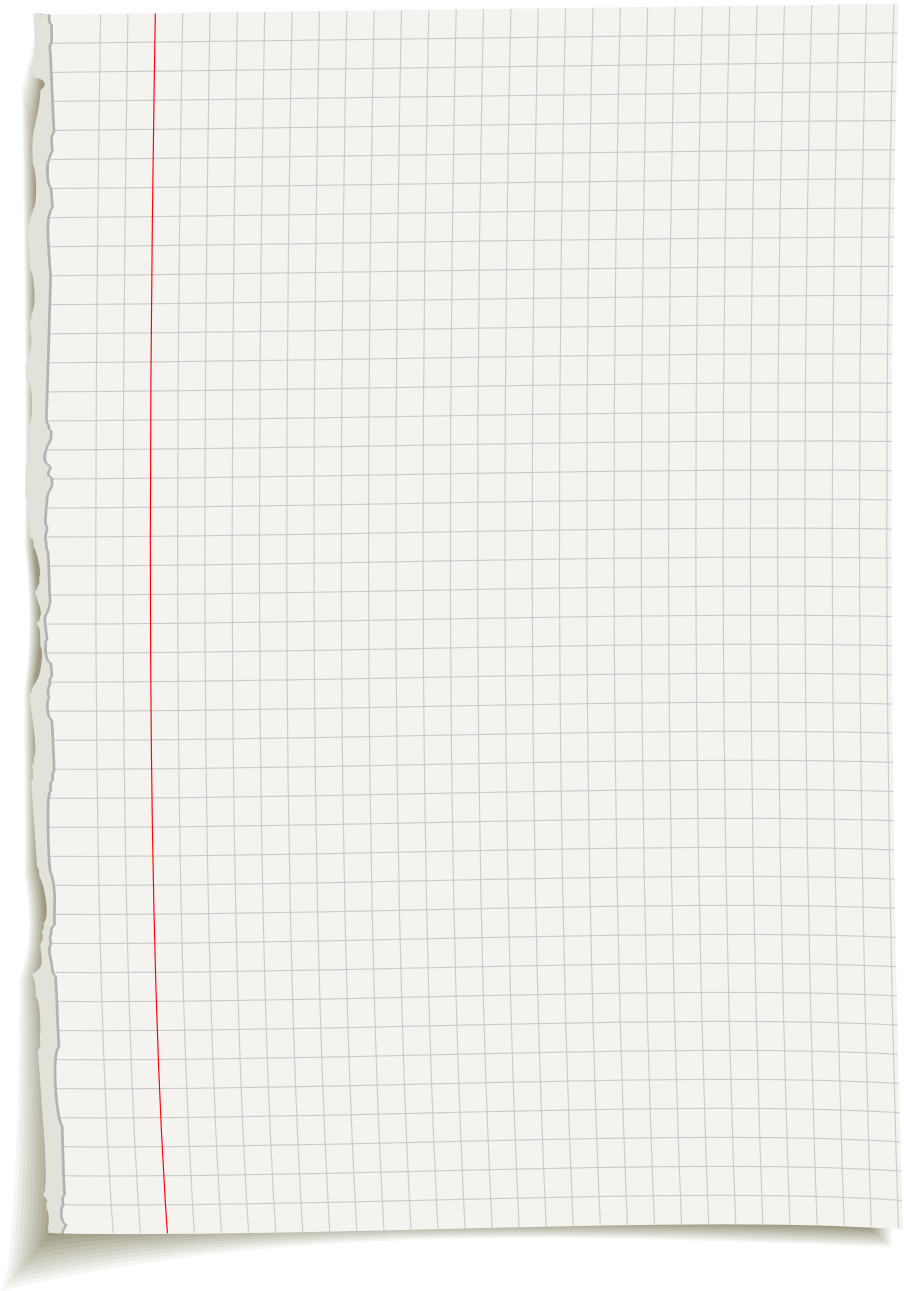
Wist je dat priemgetallen momenteel gebruikt worden om software en data te beveiligen? Een cryptograaf maakt hierbij gebruik van het product van twee hele grote priemgetallen.

Stichting FutureNL ontwikkelt onafhankelijk lesmateriaal. © 2022 Iedereen mag deze les downloaden, delen en uitprinten (alleen niet als je er geld mee wilt verdienen). Doen! Creative Commons licence: CC BY-NC-ND 4.0. Deze les is gemaakt door Sjoukje Wisman en Karlijn Ballemans van WisMon.

OPDRACHT 3 – Kraak de sleutel

Wissel jullie beveiligingssleutel uit met een ander groepje. Let op: geef alleen de sleutel, niet de twee priemgetallen!

Zelf ontvangen jullie ook de sleutel van een ander groepje. Probeer de twee priemgetallen waar deze sleutel van is gemaakt te achterhalen. Voor deze priemgetallen moet dus gelden dat ze vermenigvuldigd met elkaar gelijk zijn aan de sleutel. Hieronder vind je een kladblaadje om op te werken.



Is het gelukt om de code te kraken?

- ☐ Ja
- ☐ Nee

Zo ja, wat zijn de twee priemgetallen?

Stichting FutureNL ontwikkelt onafhankelijk lesmateriaal. © 2022 Iedereen mag deze les downloaden, delen en uitprinten (alleen niet als je er geld mee wilt verdienen). Doen! Creative Commons licence: CC BY-NC-ND 4.0. Deze les is gemaakt door Sjoukje Wisman en Karlijn Ballemans van WisMon.