Antwoorden oefenopgaven

Opgave 1
In totaal heb je 26 x 26 x 10 = 62 mogelijkheden per positie in het wachtwoord. Zodoende zijn er $62^{10} \approx 8{,}39299 \cdot 10^{17}$ mogelijke wachtwoorden.

Opgave 2
WEONTMOETENHETVIERDEUURINDEAULA

Opgave 3
Alice en Bob weten beide dat p = 31 en g = 2
Alice kiest een random heel getal, bijvoorbeeld 8 (dit is a) en berekent A met g^a mod p:
2^8 mod 31 = 8 (dit is A). A dit nu dus toevallig hetzelfde als a.
Bob kiest ook een random heel getal, bijvoorbeeld 14 (dit is b) en berekent B met g^b mod p:
2^{14} mod 31 = 16. B is dus 16.
Alice stuurt A (dus 8) naar Bob. Bob berekent A^b mod p: 8^{14} mod 31 = 4
Bob stuurt B (dus 16) naar Alice. Alice berekent B^a mod p: 16^8 mod 31 = 4
Bob en Alice hebben nu dus allebei 4 als sleutel (S).

Tip: kijk op het referentieblad op de informatica website. Daar staan enkele formules die als geheugensteuntje kunnen dienen tijdens de toets.

Opgave 4
“Virussen en wormen lijken nogal op elkaar. In de computerwereld althans. Het verschil is dat wormen zich verspreiden via internet, zonder tussenkomst van mensen. Voor een virus is altijd iemand nodig die het virus verder verspreidt. Dat kan zijn door het openen van een e-mail, of het installeren van een bestand. Of het koppelen van een USB stick (zie verderop). Maar voor zowel virussen als wormen geldt dat ze schadelijk zijn. Het verschilt zit ‘m dus in hoe het zich verspreidt, niet in wat het effect is.”

Opgave 5
HTTPS is een beveiligde vorm van HTTP en maakt gebruik van certificaten. Zo kun je achterhalen of de daadwerkelijk met de goede server contact hebt en zijn de gegevens die je verstuurt en ontvangt versleuteld.

Opgave 6
Met een webcertificaat kan een website zichzelf identificeren. In een webcertificaat staat bij welk domein het certificaat hoort en hoe lang het geldig is. Daarnaast controleert je browser ook of het niet voortijdig is ingetrokken. Een certificaat wordt uitgegeven door een certificaatuitgever. Deze zet zijn waarmerk in het uitgegeven certificaat. Die certificaatuitgever heeft zelf ook weer een certificaat van een (hogere) uitgever. Uiteindelijk zijn alle certificaten terug te voeren op een klein aantal stamcertificaten dat al in je browser is verwerkt.

Opdracht 7
Een dictionary attack is een hackpoging waarbij men probeert in te loggen met behulp van een lijst waarschijnlijke wachtwoorden. Niet alle combinaties worden uitgeprobeerd, maar een lijst waarover is nagedacht. Dit kunnen nog steeds duizenden wachtwoorden zijn, maar in ieder geval een stuk minder dan alle mogelijke combinaties.

Opdracht 8 - dit is één van de mogelijke uitwerkingen

Gegeven zijn p = 13 en q = 19:

n = 247
K = 12x18 = 216

216 = 2 x 2 x 2 x 3 x 3 x 3

d mag dus zijn: 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35, …
We nemen voor het gemak 5

e vinden we als volgt: (d x e) mod K = 1. Dus (5 x e) mod 216 = 1. Getallen die mod 216 congruent zijn aan 1, zijn producten van 216 en dan 1 erbij opgeteld. Vervolgens zoeken we een dergelijk getal dat ook nog eens deelbaar is door 5. Dit kan o.a. met een tabel, ook op je GR:

X: 1 tot …	Y1: X * 216 + 1	Y2: Y1/ 5
1	217	43,4
2	433	86,6
3	649	129,8
4	865	173
5	1081	216,2
6	1297	259,4
7	1513	302,6
8	1729	345,8
9	1945	389
10	2161	432,2
11	2377	475,4
12	2593	518,6
13	2809	561,8
14	3025	605
15	3241	648,2

Alle getallen in kolom B zijn mod 216 congruent aan 1. Met kolom C kunnen we vinden welke getallen er deelbaar zijn door 5 (al kun je dat natuurlijk ook al gemakkelijk zien aan de getallen in kolom B), namelijk 865, 1945, 3025, enz. Hierbij hoort respectievelijk een e van 173, 389 en 605.

We kunnen voor e dus 173 nemen, want (173 x 5) mod 216 = 1

De sleutels zijn dus (5, 247) en (173, 247)

Versleutelen van het getal 55: 55^5 mod 247 = 139 (reken uit met MOD_EXP op je GR)
Ontcijferen van 139: 139^{173} mod 247 = 55 (reken uit met MOD_EXP op je GR)

Opgave 9 - dit is één van de mogelijke uitwerkingen
p = 53
q = 97

n = 5141
K = 4992

4992 = 2 x 2 x 2 x 2 x 2 x 2 x 39
d mag zijn 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31, 33, etc.
Laten we d = 15 nemen

Dan geldt (15 x e) mod 4992 = 1. Om e te vinden, maken we gebruik van een tabel:

Tellen van 1 tot …	Kolom A x 4992 + 1	Kolom B gedeeld door 15
1	4993	332,866666666667
2	9985	665,666666666667
3	14977	998,466666666667
4	19969	1331,26666666667
5	24961	1664,06666666667
6	29953	1996,86666666667
7	34945	2329,66666666667
8	39937	2662,46666666667
9	44929	2995,26666666667
10	49921	3328,06666666667
11	54913	3660,86666666667
12	59905	3993,66666666667
13	64897	4326,46666666667
14	69889	4659,26666666667
15	74881	4992,06666666667
16	79873	5324,86666666667
17	84865	5657,66666666667
18	89857	5990,46666666667
19	94849	6323,26666666667
20	99841	6656,06666666667

Er lijkt geen e te zijn die hieraan voldoet. We kiezen een andere d = 17 en maken een nieuwe tabel:

Tellen van 1 tot …	Kolom A x 4992 + 1	Kolom B gedeeld door 17
1	4993	293,705882352941
2	9985	587,352941176471
3	14977	881
4	19969	1174,64705882353
5	24961	1468,29411764706
6	29953	1761,94117647059
7	34945	2055,58823529412
8	39937	2349,23529411765
9	44929	2642,88235294118
10	49921	2936,52941176471
11	54913	3230,17647058824
12	59905	3523,82352941176
13	64897	3817,47058823529
14	69889	4111,11764705882
15	74881	4404,76470588235
16	79873	4698,41176470588
17	84865	4992,05882352941
18	89857	5285,70588235294
19	94849	5579,35294117647
20	99841	5873

We kunnen voor e dus o.a. 881 kiezen

Sleutels zijn dus (17, 5141) en (881, 5141)

Versleutelen van het getal 121: $121^{17} \bmod 5141 = 4568$ (reken uit met MOD_EXP op je GR)
Ontcijferen van 4568: $4568^{881} \bmod 5141 = 121$ (reken uit met MOD_EXP op je GR)