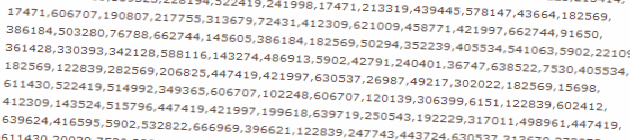
**Geocache-Beschreibung (Listing):**

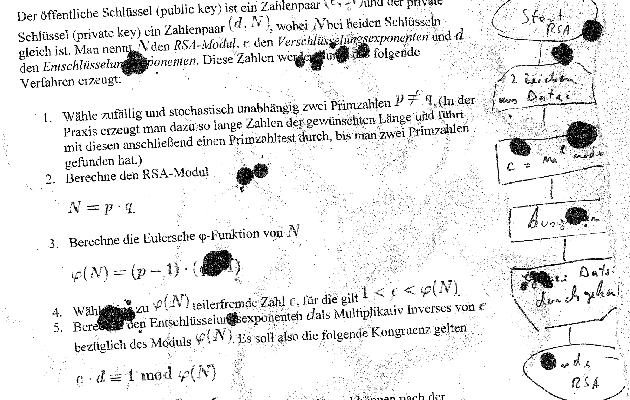
Mathematik- / Statistik- / Programmieraufgabe.  
Die Bilder, der Text und die Buchreferenz enthalten keine versteckten Informationen außer den offensichtlichen. Das Buch muss nicht zur Lösung gekauft werden (aber ich fand es interessant zu lesen).  
Die mit (\*) markierten Zahlen dienen der Orientierung worauf ihr euch schlimmstenfalls einlassen müsst, sind für die eigentlich Lösung aber unerheblich. Schnellere und geschicktere Lösungen wie die "totale brutale" wurden schon gefunden!

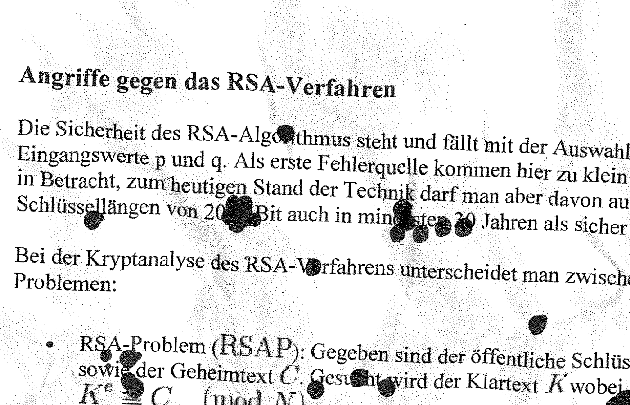
Es waren jetzt drei Tage in Folge in denen Agent Gethro Jibbs die Wohnung überwachte, aber immer noch keine Spur von dem Verdächtigen. Das war jetzt genug, sein Ziel würde nicht wiederkommen. Er hat die Chance verpasst. Sein Gegner hat seine Informationen übermittelt und sich abgesetzt, dessen war sich Agent Jibbs sicher.



Jetzt geht es nur noch um die Sicherung der Informationen die sich vielleicht finden lassen. Die Nachricht die aus der Wohnung als Mail versendet wurde konnte abgefangen werden. Er hatte sie seit Tagen vor Augen, aber außer einer Menge Zahlen konnten alle Spezialisten und Rechner in der Zentrale nicht erkennen was es damit auf sich hatte. Allen war klar dass die Nachricht Informationen über das nächste Ziel des Spions enthalten würde, und dass er in seiner üblichen geringschätzigen Art für die Arbeit seiner Verfolger in Klartext in seiner deutschen Muttersprache über das Ziel schreiben würde.

Da Jibbs bereits vorher wusste gegen wen er ermittelt, und dass diese Zielperson ein Meister der elektronischen Kriegsführung sein soll hatte er sich schon vorher Unterstüzung durch das Hauptquartier zusichern lassen. Und nun stand er hier, mit dem ihm zugeteilten Special Agent Gimothy McTee, in den Räumen die sein Ziel einige Tage als Unterschlupf gewählt hat.

Die Wohnung war praktisch leer, außer den üblichen Möbel fand sich nichts Bemerkenswertes. Nur einige zusammengeknüllte, schlecht fotokopierte und mit Flecken überzogene Seiten mit Mathematik. Für Agent Jibbs völlig unnütz, aber McTee konnte nach ein wenig querlesen erkennen um was es sich handelt: "*Albrecht Beutelspacher: Geheimsprachen. Geschichte und Techniken*", sagte er, "*Standardliteratur in der Verschlüsselungsausbildung*". Speziell in dem Abschnitt über das RSA-Verfahren waren interessante Kritzeleien am Rand. Agent Jibbs überlies die Blätter seinem Begleiter: "*Ergibt das einen Sinn?*"  
  
McTee nickte: "*Ja, das ist RSA, praktisch unknackbar. Wenn er ein gutes Programmpaket verwendet hat sind wir chanchenlos. Wir haben ja nicht mal die Zertifikate seines öffentlichen Schlüssels. Und selbst wenn... keine Chance.*"  
McTee blätterte noch etwas hin und her... "*Hm, erinnerst du dich an die Nachricht? Dass sie sehr ungewöhnlich war? Ich denke ich weiß jetzt warum. Es wurde nicht wie üblich ein hybrides Verfahren verwendet, also die eigentliche Nachricht mit einem symetrischen Verfahren und dem Schlüssel dazu mit RSA... Nein, er hat die GANZE NACHRICHT mit RSA kodiert, immer zwei ASCII-Zeichen hintereinander zusammengefasst und dann gleichzeitig codiert. Bestimmt haben die sogar alle Umlaute und Satzzeichen einfach so übernommen, oder bei den Treffpunkt-Koordinaten das ° und ' Zeichen. So etwas habe ich noch nie gesehen.*"  
"*Was hilft uns das?*" konnte Jibbs gerade noch heraus bringen bevor McTee weiter sprach: "*Völlig egal - ob du dieses oder jenes codierst. Einen Schlüssel von 2048 Bit kann kein Rechner in keiner Zeit knacken. Und wie gesagt, selbst wenn, wir hätten diesen Schlüssel ja noch nicht einmal.*"



Agent Jibbs hatte die Blätter zwischenzeitlich noch mal überflogen. "*Das stimmt wohl. Aber ist dir das schon aufgefallen?*" McTee stutzte. "*Nein. Aber SO blöd kann unsere Zielperson nicht sein. Niemals. Wobei... wer so überheblich ist sein eignes Programm zu bauen... Vielleicht hat er das Verfahren wirklich nicht verstanden? Das wäre ja überaus originell wenn ein paar Regentropfen auf einem schlechten Ausdruck dafür sorgen dass er an dieser Stelle sein Programm falsch aufbaut.*"  
Jibbs wurde hellhörig: "*Ich will Antworten. Wenn es eine Möglichkeit gibt, wie lange wird das dauern?*"  
McTee war verunsichert. "*Es gibt immer noch 29584 (\*) Kombinationen. Oder nein eigentlich nur 14878 (\*). Wobei... ja, es sind nur 14706 (\*).  
Aber dann für die dritte Variable der Verschlüsselng jedesmal mehrere tausend oder sogar zehntausende, hunderttausende Möglichkeiten. Aber ich gehe sofort ins Labor und arbeitete daran.*"

Zwei Tage später klickten die Handschellen. Agent Jibbs nickte McTee zu: "*Verstanden habe ich es nicht, aber egal. Die Koordinaten des Übergabepunktes stimmten jedenfalls. Gute Arbeit!*"  
"*Wir hatten Glück. Das Programm hat den Treffer schon nach wenige mehr als der Hälfte der Möglichkeiten gefunden, und selbst das hat fast 20 h (\*) gedauert.*" konnte McTee noch erwidern, wurde aber von Jibbs lachen unterbrochen: "*Warum soll man nicht auch mal Glück haben.*"

Noch ein paar Hinweise: Die schlechten Bilder sind natürlich Absicht. Der Meisterverbrecher war eben sparsam und hat schlechte Kopien statt einem Original verwendet. Die Wasserflecken sind rein zufällig... fast alle... Nur einer ist an einer genau absichtlich plazierten Stelle.  
Die Formeln besorgt ihr euch besser woanders komplett lesbar, die verdeckten Teile sind zwar richtig aber eben nicht komplett.

Und noch ein paar Details in Fachsprache:  
p und q jeweils prim  
e und d teilerfremd, phi und e teilerfremd, phi und d teilerfremd  
e "überschaubar" groß. d riesig.

**Vielen Dank an kaeptn\_iglu, GeoKaptn und Zysmo, brosaar und plasm für ihr Feedback und Korrekturen!**

541063,5902,221098,530175,412309,304532,413019,366245,5902,344890,247743,36747,638522, 7530,405534,214405,514992,434897,104250,304532,290894,262763,275690,5902,434897,343845, 477510,159878,592665,419234,182569,445999,172995,5902,182569,306123,47335,240401, 417428,356479,7530,203026,275690,20039,412309,641226,98778,458771,275690,88000,412309, 532822,242246,247743,20039,154187,660872,273541,486913,91650,386184,6151,586529,139190, 577855,403050,412309,197513,506052,122839,392036,366245,52649,7530,405534,99660,17384, 182569,154187,579451,143274,207070,581096,471659,573821,63666,576241,215414,372905, 421997,660872,363230,313679,268348,306399,52649,619009,88711,163321,182569,490648, 306399,639719,418396,7530,26987,47335,306399,120139,306399,469173,447741,155744,20039, 147239,5902,447419,515796,36747,638522,7530,197513,51252,18979,183309,108225,215414, 617126,282589,359323,228194,522419,241998,17471,213319,439445,578147,43664,182569, 17471,606707,190807,217755,313679,72431,412309,621009,458771,421997,662744,91650, 386184,503280,76788,662744,145605,386184,182569,50294,352239,405534,541063,5902,221098, 361428,330393,342128,588116,143274,486913,5902,42791,240401,36747,638522,7530,405534, 182569,122839,282569,206825,447419,421997,630537,26987,49217,302022,182569,15698, 611430,522419,514992,349365,606707,102248,606707,120139,306399,6151,122839,602412, 412309,143524,515796,447419,421997,199618,639719,250543,192229,317011,498961,447419, 639624,416595,5902,532822,666969,396621,122839,247743,443724,630537,313679,273073, 611430,20039,7530,338990,532822,389080,447419,221098,523487,182569,616131,5902,363423, 228194,396599,422378,122451,405534,112161,577855,403050,412309,197513,423345,122839, 407563,154389,126217,108225,215414,108225,447741,100276,217755,313679,16539,365434, 606707,436324,404035,77820,297552,641226,43921,361428,545814,532822,242246,247743, 20039,275690,20039,143274,232606,59008,20039,414117,100276,539474,458771,158565,275690, 6151,405534,616131,532822,12625,228194,122839,412309,580207,412309,20039,389080,283493, 308979,458771,192229,7530,306399,532822,51252,52649,340710,5902,498961,120139,306399, 6151,279179,447419,319809,215414,522419,182569,442052,306399,221098,639719,98778, 311405,363423,458771,430166,639719,120139,306399,434897,130307,340710,498961,578147, 514992,275690,5902,639719,630537,466629,125906,331358,610026,170359,182569,154941, 26987,308182,313679,42791,5902,498961,20039,541063,5902,221098,487491,211869,444993, 192229,41223,594596,313679,26987,498961,43921,142588,352239,147239,154389,306123, 515178,577855,639719,289363,591897,363423,43921,421997,100276,242628,10460,434897, 649867,120139,306399,522419,182569,154389,539474,20039,170359,182569,616131,639719, 447419,221098,6151,413019,182569,147239,494025,514992,217755,221098,471659,610026, 206825,444607,412309,529972,524991,524991,541063,5902,221098,329682,421997,8133,6151, 586529,666969,221098,54852,415821,421997,20039,389080,447419,221098,189140,421997, 363230,444993,262763,363230,405534,154187,660872,424692,142025,421997,405534,78896, 76788,50294,352239,576241,447854,643403,67067,412309,303628,434897,586529,112161, 577855,546286,306399,447419,182569,630537,587921,3978,158565,375321,361428,363230, 313679,67067,412309,501345,52649,7530,405534,420609,340710,188587,182569,304532,396095, 327588,639719,361428,545814,532822,404035,515178,477008,154187,660872,594596,313679, 8002,7530,523487,221098,405534,266180,662744,602272,221098,530175,506052,215414,532822, 51252,396095,243122,532822,375321,275690,5902,221098,189140,421997,363230,413542, 7530,26987,120139,306399,189140,421997,363230,290894,447854,313679,292674,96254,532822, 616131,532822,205621,363230,59008,221098,602412,26987,660872,262763,36747,638522, 7530,405534,262763,661977,221098,193716,306399,532822,268348,306399,52649,619009, 88711,221098,361428,515252,7530,469173,3978,50294,221098,532822,661977,507569,182569, 532822,242246,632592,498961,602412,26987,660872,317701,520846,530175,634725,419234, 3978,275632,43690,530175,43481,275690,442052,327588,530175,419609,59008,530175,165266, 607868,7530,228194,47335,135214,638522,526292,471659,458771,515178,354445,530175, 632714,35837,581096,649867,221098,530175,435915,240401,192229,41223,47633,3978,17384, 221098,221423,576241,447854,122839,42791,5902,333704,51669,530259,444993,221098,120139, 306399,418396,293645,290894,514992,660872,254781,430166,532822,13037,630363,182569, 47335,306399,94571,361428,458366,596823,577855,515796,469173,458771,580207,20039, 541063,5902,221098,6151,586529,112161,577855,221098,120139,306399,439445,122839,221098, 434897,405534,412309,641226,405534,122839,632592,494025,52649,7530,405534,214141, 577855,192229,105547,154187,579451,546286,331131,530175,389080,447419,515796,447419, 421997,662744,145605,386184,532822,17362,590218,263807,221098,546286,265044,530175, 302725,638522,278488,201198,154389,332817,182569,518073,36747,206825,275632,43690, 530175,616766,639719,506052,446071,182569,120139,306399,617126,508492,18979,154389, 405534,614586,577855,366245,5902,530175,209189,5902,506052,446071,182569,417137,3205, 320398,122839,366245,5902,120139,306399,662744,292169,371343,182569,589057,665171, 250543,192229,41223,363230,100276,242246,247743,20039,304532,50047,458771,515060, 524991,524991,162909,100276,541063,5902,221098,182569,331358,241998,530175,594596, 313679,592665,279179,193716,192229,7530,405534,541063,5902,221098,32305,120139,306399, 447419,182569,331358,241998,52649,619009,183309,199618,76788,363230,405534,515935, 354340,434897,206825,465876,486913,498961,313679,363230,338990,52649,7530,313679, 273541,104250,76788,363230,285157,282569,477008,154187,660872,375321,412309,498961, 313679,273541,104250,76788,363230,285157,282569,477008,506052,104250,506052,215414, 6151,405534,616131,532822,423345,104250,182569,143274,366245,122839,532822,363230, 100276,301788,106534,487277,434897,575018,304532,139190,15313,221098,361428,541063, 5902,221098,6151,122839,344890,275690,5902,354885,419234,215414,304212,576241,215414, 447419,182569,418396,364762,334779,35837,43690,331729,20039,541063,5902,221098,588116, 143274,100276,412309,641226,447419,182569,469173,168047,351105,221098,120139,306399, 636596,546286,616131,494025,514992,396599,412309,5902,122839,221098,636596,409008, 302022,275690,5902,221098,51669,206218,317011,5902,311405,221098,630537,76788,588974, 245490,530175,616131,532822,18979,215414,17471,606707,185350,266180,418396,197531, 122451,405534,363230,100276,340229,193716,430166,221098,207070,501345,494025,142588, 207336,532822,304532,545244,577855,182569,20039,96254,577855,461388,145351,147705, 182569,259369,192229,7530,405534,289061,230838,19914,154187,52649,24710,617126,221098, 405534,553614,158565,275690,154941,421997,100276,154389,18979,405534,603072,59008, 498961,122839,447419,262763,405534,619009,122839,447419,433860,363230,405534,420609, 611430,545949,18979,477008,49217,611430,469173,188587,154187,363230,153537,617126, 245490,447419,282589,417137,76788,296027,447741,104250,602412,26987,660872,616131, 532822,64994,3205,616131,147239,498961,295701,524991,411369,495382,78367,81952,298041, 240023,630537,497527,17276,78367,473584,281325,317051,524991,43481,98778,262763,126217, 20039,412309,405534,157091,279179,193716,469917,434897,405534,363230,405534,64994, 3205,616131,147239,498961,405534,363230,313679,513944,428789,613304,412309,5902,221098, 313679,315022,580207,469173,338990,296027,508492,465876,26987,208493,532822,503155, 215414,434897,434240,498961,430166,221098,530175,412309,405534,282569,607868,309123, 217755,465876,226509,245490,108225,142588,52649,340710,304532,100276,149244,315022, 228194,329682,421997,8133,447419,282589,631539,20039,304532,304532,195945,143274, 47861,524991,524991,410604,3978,221098,331358,262763,497630,414117,418940,313679, 96268,18979,405534,154187,660872,638870,3978,662744,666295,503101,143274,266180,662744, 246302,7530,153537

Hinweis: http://de.wikipedia.org/wiki/RSA-Kryptosystem