Kryptographie – Letterbox

Diese Letterbox besteht aus 3 Teilen, welche jeweils in mehrere Teile untergliedert sind. Du solltest dir als etwas Zeit nehmen. :-)

Teil 1 besteht aus zwei Teilen: der erste Teil gibt dir einen Lösungshinweis um im zweiten Teil den Homepagenamen herausfinden zu können.
Teil 2 besteht aus drei Teilen: der erste Teil bildet die Grundlagen und gibt dir einen Hinweis um das Geheimnis im zweiten Teil herausfinden zu können, dass dich im dritten Teil zum Benutzernamen führt.
Teil 3 besteht aus vier Teilen: im ersten Teil findet man eine Lösung, diese muss mit einem Teilergebnis aus dem zweiten Teil im dritten Teil entschlüsselt werden. Und anschließend im vierten Teil mit dem zweiten Teilergebnis aus dem zweiten Teil umgewandelt werden um am Ende das Passwort zu erhalten.

Hinweis zum Lösen dieses Rätsels: ä = ae, ö = oe, ü = ue, ß = ss

Viel Spaß beim Knacken der Codes!

Teil 1: Der Homepagename

Löse das Texträtsel in Teil a) um an einen Hinweis zu kommen, welcher dir hilft, den Code aus Teil b) zu knacken. Die Zahlen dahinter geben dir an, welchen Buchstaben du an welche Stelle des Lösungswortes setzen musst.
1-4 bedeutet: Der erste Buchstabe des Wortes ist der vierte Buchstabe des Lösungswortes.

---

a) Die Kryptographie war ursprünglich die Wissenschaft der _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ (2-4). Heute befasst sie sich allgemein mit dem Thema _ (4-10).

Das Ziel ist, die _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ (6-8) einer Nachricht zu gewährleisten, also sicherzustellen, dass eine dritte Person die Nachricht nicht lesen kann.

Hierzu wird die eigentliche Nachricht, auch _ _ _ _ _ _ _ _ (2-6) genannt, nach einer bestimmten Logik verschlüsselt. Die verschlüsselte Nachricht heißt _ _ _ _ _ _ _ _ _ _ _ (6-3), und sieht auf den ersten Blick wie kompletter Unsinn aus.

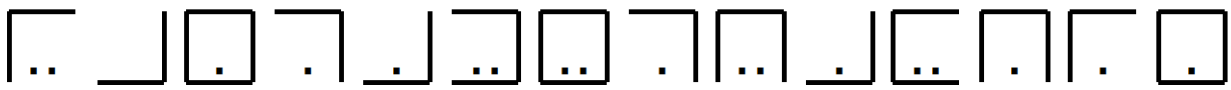
Die einfachste Verschlüsselung ist die sog. _ (18-9), bei der jeder Buchstabe des Alphabets durch je einen anderen Buchstaben, Zahl oder Zeichen ersetzt wird.

Bereits der römische Kaiser _ _ _ _ _ _ _ _ _ _ _ _ _ _ (1-1) verwendete eine Art dieser Verschlüsselungen um seine militärischen Befehle geheim zu halten. Die Art der Verschlüsselung, welche er verwendete, war ein einfaches _ _ _ _ _ _ _ _ _ _ _ _ (11-11) des Alphabets und kann leicht geknackt werden. Man benötigt maximal 26 Versuche um den Code durch Ausprobieren zu knacken.

Schnell wurden statt Buchstaben auch Zeichen verwendet, um die Verschlüsselung sicherer zu machen. Der Nachteil ist jedoch, dass meist sehr lange Texte damit verschlüsselt wurden. Eine Verschlüsselung ist umso sicherer, je _ _ _ _ _ _ _ (3-7) der zu verschlüsselnde Text ist. Einen _ _ _ _ _ _ (2-2) Text kann man mit einer _ (12-5) knacken, denn bestimmte Buchstaben kommen in der Sprache häufiger vor als andere.

1	2	3	4	5	6	7	8	9	10	11

b) Löse nun mit dem Hinweis aus Teil a) folgende Verschlüsselung um den Homepagenamen herauszufinden.



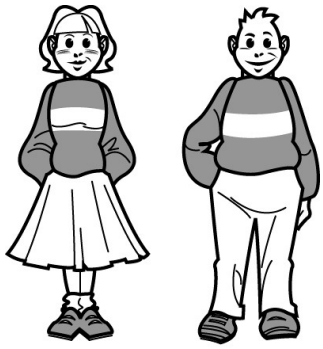
www. _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ .de.tl

Teil 2: Der Benutzername

Löse den Lückentext um an das Lösungswort zu kommen, welches du für Teil b) benötigst. Die Zahlen dahinter geben dir auch hier an, welchen Buchstaben du an welche Stelle des Lösungswortes setzen musst.
1-4 bedeutet: Der erste Buchstabe des Wortes ist der vierte Buchstabe des Lösungswortes.

---

a) Alle Verfahren, bei denen sowohl Empfänger als auch Absender einer Nachricht, denselben Schlüssel verwenden, heißen _ _ _ _ _ _ _ _ _ _ _ _ _ (8-3) Verfahren. Diese Verfahren können von heutigen Computern sehr schnell berechnet werden, weil alle notwendigen Berechnungsschritte in der _ _ _ _ _ _ _ _ (2-6) berechnet werden können. Aber diese Verfahren haben einen gewaltigen Nachteil: den _ (6-1), denn dieser muss über einen unsicheren Weg geschehen und kann dabei von einem Dritten, dem sog. _ _ _ _ _ _ _ _ _ _ _ _ _ _ (1-5), abgefangen werden, der dann jede Nachricht entschlüsseln kann.



Alice und Bob möchten sich verschlüsselte Nachrichten schicken, hierzu möchten sie eine Alphabet-Verschiebung nach rechts verwenden. Jetzt stehen beide vor dem Problem: wie einigen sie sich auf einen sicheren Schlüssel, den außer ihnen beiden keiner kennt?

Nach kurzer Internet-Recherche einigen sich beide auf den _ _ _ _ _ _ _ - _ _ _ _ _ _ _ _ - Schlüsselaustausch (13-2). Hierzu einigen sich Alice und Bob zunächst auf eine Zahl g, diese Zahl heißt _ _ _ _ _ _ _ _ (6-4). Zudem einigen sie sich auf die Restklasse „mod p“. Diese beiden Parameter brauchen nicht geheim zu bleiben, daher einigen sie sich auch gleich auf g = 5 und p = 47.

Restklasse? Klingt kompliziert? Glaube mir, ist es nicht. :-)

In der Schule schrieb man
13 : 3 = 4 Rest 1
14 : 3 = 4 Rest 2

heute schreiben wir
$13 \equiv 1 \bmod 3$
$14 \equiv 2 \bmod 3$
(lies: 13 ist kongruent 1 modulo 3)
Bedeutet nichts anderes, als: Wenn ich 1 durch 3 teile erhalte ich denselben Rest, wie wenn ich 13 durch 3 teile.

Gar nicht so schwer, oder? Also weiter...

Alice wählt dann eine Zahl a, die nur sie kennt und veröffentlicht die Zahl $A = g^a \equiv 11 \bmod p$.
Bob wählt ebenso eine Zahl b, die nur er kennt und veröffentlicht die Zahl $B = g^b \equiv 12 \bmod p$.
Die Zahlen a und b bleiben geheim.

Der geheime Schlüssel K ergibt sich nun aus $K = A^b$ bzw. $K = B^a$. Da wir als dritter aber nicht wissen, welche Zahlen a und b Alice und Bob gewählt haben, kommen wir hier erst mal nicht weiter.
Da Alice sowohl B kennt, weil Bob es veröffentlicht hat, als auch ihr eigenes a, kann sie K berechnen, Bob natürlich ebenfalls. Ein Dritter – so wie wir - kann es nicht, da ihm die geheime Information fehlt.

Mit diesem geheimem Schlüssel K können beide nun ihre Nachrichten durch eine Alphabet-Verschiebung um K nach rechts verschlüsseln – und natürlich durch Verschiebung nach links auch entschlüsseln. („nach rechts“ bedeutet bei einer Verschiebung um 1: aus A wird B).

Teillösung:

1	2	3	4	5	6

b) Bob hat mir jedoch einen Tipp gegeben um an seinen geheimen Schlüssel zu kommen.

Wandle nun jede Zahl des Lösungswortes aus Teil a) in Zahlen um (A = 1, B = 2, ...). Bilde die Summe.

_ + _ _ + _ + _ + _ _ + _ = _ _

Bilde nun die Quersumme des Ergebnisses

_ _

und ziehe von dieser 3 ab.

_ _

Nun musst du mir glauben: Wir haben das Geheimnis von Bob.

b = _ _

Dank dieses Geheimnisses können wir nun ganz einfach den Schlüssel K berechnen. Danke, Bob!

K ≡ _ _ mod p

c) Da wir nun den Schlüssel K kennen, können wir den Benutzernamen, welchen Alice verschlüsselt geschickt hat, entschlüsseln.

Z	E	Q	D	S	B	Q	H	A	U

Herzlichen Glückwunsch, du hast den Benutzernamen erhalten!

Teil 3: Das Benutzerkennwort

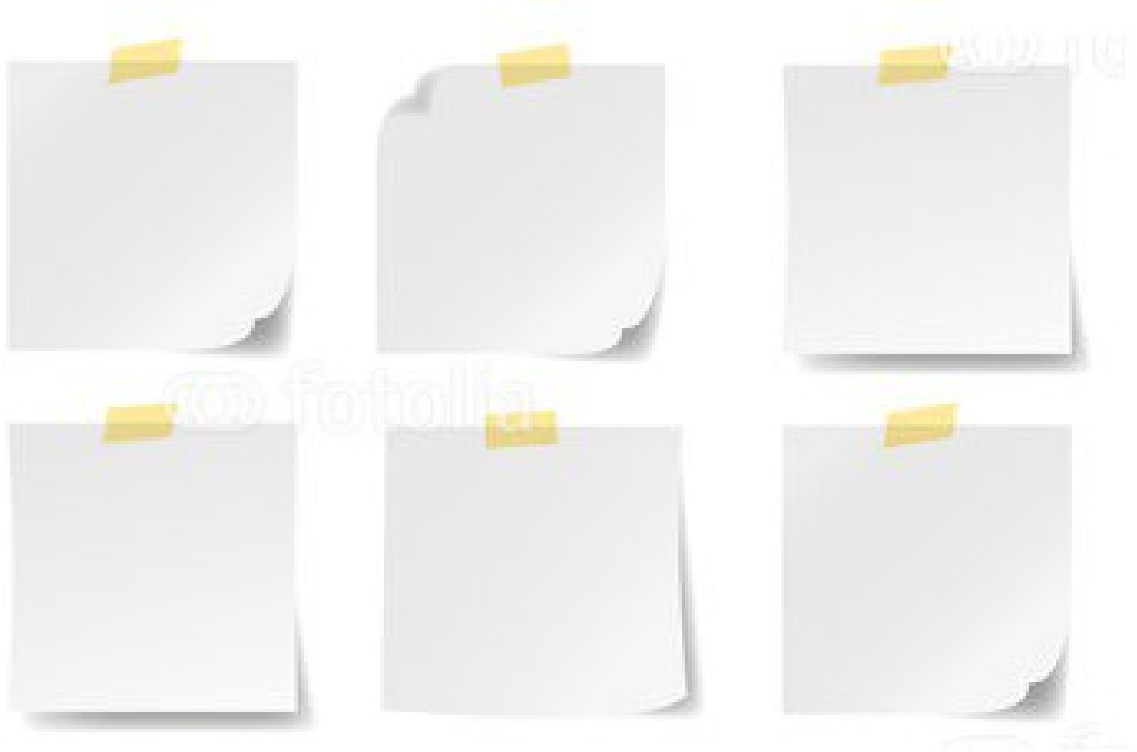
Löse den Lückentext in Teil a) um an das Lösungswort zu kommen, welches du mit dem Schlüssel aus Teil b) in Teil c) entschlüsseln kannst um dann in Teil d) mit Hilfe eines zweiten Lösungswortes aus Teil b) an das Passwort für die Homepage zu gelangen. Die Zahlen dahinter geben dir hier an, welcher Buchstabe für das Lösungswort benötigt wird – Teilweise stehen hier aber auch andere Anweisungen. Daher bitte genau lesen!

---

a) Neben den Verfahren aus Teil 2 gibt es natürlich auch die _ _ _ _ _ _ _ _ _ _ _ _ _ _ (14) Verfahren. Hier verwenden Absender und Empfänger unterschiedliche Schlüssel. Diese Verfahren haben kein Problem beim Schlüsselaustausch. Aber sie haben dafür einen anderen Nachteil, denn diese Verfahren sind vergleichsweise _ _ _ _ _ _ _ (4), da die Logik komplett in der _ _ _ _ _ _ _ _ (Buchstabe 4 als Zahl minus Buchstabe 1 als Zahl, Ergebnis als Zahl) realisiert werden muss. Das bekannteste dieser Verfahren ist der sogenannte RSA-Algorithmus.

Möchte Bob eine Nachricht an Alice schicken, so benötigt er dafür nur den _ _ _ _ _ _ -Key (3) von Alice für die Verschlüsselung der Nachricht. Dieser Schlüssel ist ein Zahlenpaar (e, N) = (7, 33). Alice kann dann mit ihrem _ _ _ _ _ _ _ -Key (Buchstabe 3 als Zahl plus Buchstabe 7 als Zahl, Ergebnis in Buchstabe), welchen nur sie kennt, die Nachricht entschlüsseln. Auch dieser Schlüssel ist ein Zahlenpaar (d, N). Das N ist in beiden Schlüsseln gleich und wird RSA-_ _ _ _ _ (2) genannt. N ist hierbei stets das Produkt aus zwei Primzahlen. Die Zerlegung ist daher eindeutig, d ist der geheime Teil, den nur Alice kennt.

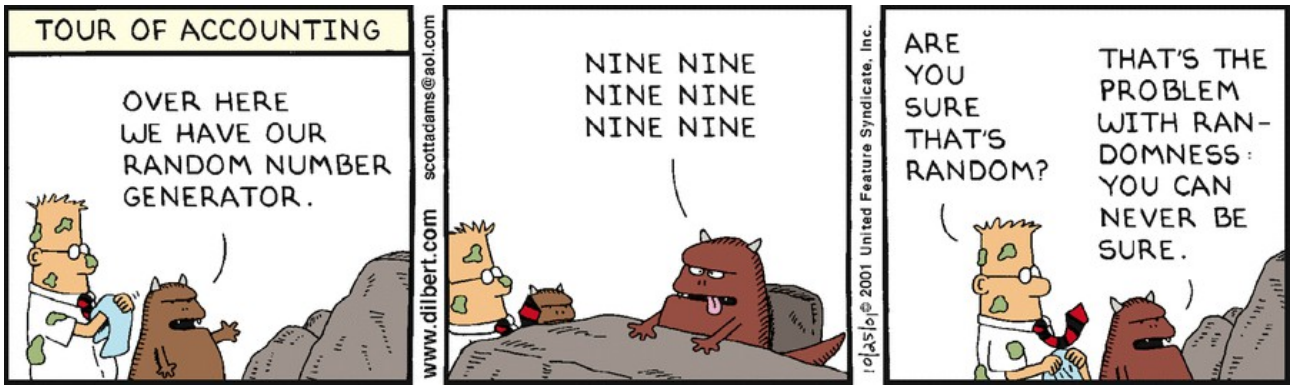
Leider kam die Lösung von Bob an Alice zu allem Überfluss nicht nur verschlüsselt, sondern auch noch zerrissen an. Aber du hast nun immerhin alle 6 Zeichen erhalten. Trage sie hier ein.



b) Wenn es gelingt die _ (18-4) von N zu knacken, so kann die Verschlüsselung geknackt werden. Daher werden in der Praxis sehr _ _ _ _ _ _ (4-6) Primzahlen verwendet um eine Faktorisierung nahezu unmöglich zu machen. Bei _ _ _ _ _ _ _ (4-5) Primzahlen sieht man die Lösung entweder sofort oder kann sie durch Probieren, in der Fachsprache _ _ _ _ _ _ _ _ _ _ (6-1) Methode genannt, herausfinden.

Selbst moderne Computer benötigen viele _ _ _ _ _ _ _ _ _ _ _ (5-2) Jahre um alle Möglichkeiten durchzuprobieren. Erst die Entwicklung der _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ (8-7) könnte diesen Algorithmus gefährden.

In der Praxis werden Primzahlen für RSA-Algorithmen jedoch als _ _ _ _ _ _ _ _ _ _ _ _ _ _ (13-3) generiert. Und diese Algorithmen sind angreifbar und bilden die große Sicherheitslücke in der RSA-Verschlüsselung.



In unserem Beispiel ist die Verschlüsselung leicht zu knacken, da Alice zwei sehr kleine Primzahlen gewählt hat. Knacke daher die Verschlüsselung.

$$N = p \cdot q = \_ \cdot \_\_$$

Da wir nun die beiden Primzahlen kennen, können wir die _ _ _ _ _ _ _ _ _ _ (8-8) Phi-Funktion berechnen.

$$\varphi(N) = (p-1)\cdot(q-1) = \_ \cdot \_\_$$

Nun gilt weiter

$$\varphi(N)+1 = e \cdot d$$

Berechne mit dieser Information Alice privaten, geheimem Schlüssel d.

$$d = \_$$

Trage hier die Lösungsbuchstaben ein:

1	2	3	4	5	6	7	8

c) Die Lösung aus Teil a) kann Alice nun mit ihrem Private-Key d entschlüsseln.

Alice und Bob haben vereinbart, dass sie ein Alphabet mit 36 Zeichen verwenden (0 ist das Leerzeichen, 1 – 26 sind die Buchstaben A-Z, 27 – 36 sind die Ziffern 0-9). In der Praxis wird hier meist der ISO-Zeichensatz gewählt.

Zunächst wandeln wir das die 6 Lösungszeichen aus Teil a) in dieses Alphabet um.

Für die Dechiffrierung jedes dieser Zeichen z' gilt

$$(z')^d \equiv z \; mod \; N$$

wobei z' das verschlüsselte und z das entschlüsselte Zeichen ist. Wenn wir dies nun für alle 6 Zeichen durchführen, erhalten wir.

_ _ ⁻ ≡ _ mod _ _

_ ⁻ ≡ _ _ mod _ _

_ _ ⁻ ≡ _ mod _ _

_ ⁻ ≡ _ mod _ _

_ _ ⁻ ≡ _ mod _ _

_ _ ⁻ ≡ _ mod _ _

Wandle nun diese 6 entschlüsselten Zeichen (z) gemäß der Vereinbarung von Alice und Bob um.

In der richtigen Sortierung ergeben diese Buchstaben:

d) Aus der richtig sortierten Lösung aus Teil c) in Verbindung mit dem Lösungswort aus Teil b) erhältst du das Passwort für die Homepage.

_ _ _ _ _ _ _ _

Logge dich nun auf der Homepage ein und trage dich ins Gästebuch ein um den Stempel zu erhalten.