Kryptologie: Übungsblatt 1, Besprechung ab dem 23.4.2018, 10:15, H20

0.) Überliefert ist folgende Korrespondenz zwischen Friedrich dem Großen und Voltaire. So schrieb Friedrich an Voltaire folgende Botschaft:

$$\frac{P}{ce\ soir}\ a\ \frac{6}{100}$$

Hierauf antwortete Voltaire mit

$$G\,a$$

Können Sie das entschlüsseln?

1.) Ein deutscher Text wurde monoalphabetisch verschlüsselt und soll von Ihnen (ohne Kenntnis des Schlüssels) entschlüsselt werden:

WE JWEFZWZWR RMFZ IWXFZWR TRA NTRAWB

Um die Entschlüsselung einfacher zu machen, haben wir die Leerzeichen zwischen den Wörtern angegeben.
Ferner geben wir einige Fakten an, die bei der Entschlüsselung sicher helfen:
Die häufigsten Buchstaben im Deutschen sind:

E (17 %) $>$ N (10 %) $>$ I, R, S, T, A (6–7 %)

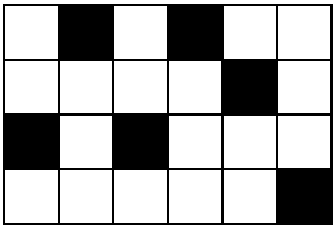
Die häufigsten Buchstabenpaare (Bigramme) im Deutschen sind: ER, EN, CH, DE, EI, ND, TE, IN, IE.

In der obigen Chiffre kommen folgende Buchstaben am häufigsten vor: W: 7-mal, R: 5-mal, Z: 4-mal, F: 3-mal, T,A,E: 2-mal, die restlichen Buchstaben 1- oder 0-mal.

In der Chiffre fallen folgende wiederholt auftretende Buchstaben-Paare oder Tripel auf: WE, ZW, WR, FZ, ZWR, TRA.

2.) Ein Cäsar-verschlüsselter deutscher Text beginnt mit NRJ.... Welches könnte der korrekte Schlüssel sein?
Experimentieren Sie mit solchen Satzanfängen. Wieviele Chiffre-Buchstaben sind typischerweise erforderlich, bis der Schlüssel mit großer Sicherheit eindeutig feststeht? (Das ist das so genannte **Unizitätsmaß** der betreffenden Chiffriermethode.)

3.) Jemand hat folgende Schablone



für eine Transpositionschiffre verwendet. Herausgekommen ist folgender Chiffretext:

R	A	A	N	G	E
F	D	R	E	K	I
O	Z	M	E	E	N
D	I	E	T	H	M

Wie wurde die Schablone verwendet und was ist der Klartext?

4.) Die Verschlüsselung bei der ENIGMA-Maschine geschieht mit Hilfe von Walzen (runde Scheiben), auf denen auf Vorder- und Rückseite kreisförmig 26 Metallstifte angeordnet sind (die die Buchstaben repräsentieren). Im Inneren der Walze sind die Stifte auf der Vorderseits gemäß einer festen Permutation aus S_{26} mit den Stiften auf der Rückseite elektrisch verbunden. Allerdings darf die in einer solchen Walze verdrahtete Permutation π keinen Fixpunkt enthalten, d.h. $\pi(x) = x$ ist nicht zugelassen. Auf wieviele Weisen kann eine Walze in zulässiger Weise verdrahtet werden?

Tatsächlich kommt noch eine weitere Forderung an die betreffende Permutation hinzu: Wenn $\pi(x) = y$ verdrahtet ist, so muss auch $\pi(y) = x$ verdrahtet sein. Dies deshalb, damit man die ENIGMA-Maschine in derselben Weise wie zum Verschlüsseln auch zum Entschlüsseln verwenden kann. Wieviele zulässige Permutationen gibt es nun bei dieser weiteren Einschränkung?

5.) Bei der affinen Verschlüsselung wird jeder Klartextbuchstabe $x \in \{0, 1, \ldots, 25\}$ der Chiffrierfunktion $(ax + b)$mod 26 unterzogen, wobei $k = (a, b)$ der Schlüssel ist, $a, b \in \{0, 1, \ldots, 25\}$. Nicht alle der $26 \cdot 26 = 676$ Schlüsseln ergeben eine injektive Funktion. Charakterisieren Sie diejenigen Schlüssel, die zulässig sind, also die auf eine injektive (sogar bijektive) Funktion von $\{0, 1, \ldots, 25\}$ nach $\{0, 1, \ldots, 25\}$ führen.

Listen Sie die zulässigen Konstanten $a \in \{0, 1, \ldots, 25\}$ explizit auf und finden Sie für jedes solche a ein geeignetes a' mit $a \cdot a' \equiv 1$ (mod 26). (Bei dieser Aufgabe ist dies eher durch Probieren gemeint; später werden wir eine systematische Methode kennenlernen.)

6.) Es wird die affine monoalphabetische Chiffrierung $c = (3x + 5)$ mod 26 verwendet (wobei c der Chiffrebuchstabe, x der Klartextbuchstabe ist). Stelle die Umkehrfunktion (also die Dechiffrierfunktion) ebenfalls als affine Funktion dar: $x = (ac + b)$ mod 26, für geeignete Konstanten $a, b \in \{0, 1, \ldots, 25\}$.

7.) Jemand kommt auf die Idee, die affine Verschlüsselung durch doppelte Verschlüsselung zu verbessern. Nachdem mit geeigneten Konstanten a_1, b_1 verschlüsselt wurde: $c_1 = (a_1 \cdot x + b_1)$ mod 26, wird mit 2 weiteren Konstanten a_2, b_2 nochmals verschlüsselt: $c_2 = (a_2 \cdot c_1 + b_2)$ mod 26. Was halten Sie davon?
Überlegen Sie sich dieselbe Frage nochmals in Bezug auf eine doppelte Vigenère-Verschlüsselung. Was ist, wenn die beiden verwendeten Schlüssel gleich lang / verschieden lang sind?

8.) Mit etwas Glück haben wir bei einer affinen Chiffrierung herausgefunden, dass I (=8) abgebildet wird auf P (=15), und dass F (=5) abgebildet wird auf Q (=16).
Bestimmen Sie den geheimen Schlüssel $k = (a, b)$.

9.) Bei einer (fortgeschrittenen Version der) ENIGMA-Maschine besteht ein Teil des Schlüssels darin, anzugeben, welche 3 von 5 zur Verfügung stehenden Walzen in die Maschine eingelegt werden sollen – und in welcher Reihenfolge (Beispiel: man gibt an 4,2,5). Anschließend wird jede der 3 eingesetzten Walzen auf einen (von 26) Buchstaben voreingestellt. (Beispiel: man gibt an: GXU). Auf wieviele Weisen kann man diese (Teil-)Schlüssel, z.B. $425GXU$, wählen? (Tatsächlich kommt noch die Angabe der Verschaltung eines Steckfeldes für die gesamte Schlüsselinformation hinzu.)

10.) Angenommen die Anzahl der Schlüssel bei einem Chiffrierverfahren sei gerade noch so erträglich groß, so dass man mit heutigen Computern alle Schlüssel k auf einen abgefangenen Chiffretext c anwenden und $D(c,k) = m$ berechnen kann. Kein Mensch kann sich solcherart Aber-Millionen potenzielle Klartexte m ansehen und entscheiden, welcher davon ein sinnvoller deutscher Text ist. Wie kann man diesen Vorgang automatisieren, so dass der Computer eine Vorauswahl treffen kann und der Mensch sich nur einige wenige m's ansehen muss?

11.) Aus einem gegebenen Text $a_1 a_2 \dots a_m$ (wobei $a_i \in \Sigma = \{A, B, \dots, Z\}$) lässt sich eine Schätzung des zugrunde liegenden Koinzidenzindex IC berechnen mittels:

$$\widetilde{IC} = \sum_{a \in \Sigma} \frac{h(a)}{m} \cdot \frac{h(a)-1}{m-1}$$

Hierbei ist $h(a)$ die Häufigkeit des Buchstabens a im Text und m ist die Textlänge. Wie kann man den $\widetilde{IC}$-Wert als Wahrscheinlichkeit bei einem bestimmten Zufallsexperiment interpretieren?
Bei einem zufälligen, auf Σ gleichverteilten Text, wird dieser Schätzwert mit hoher Wahrscheinlichkeit kleiner als 5 % sein, bei einem deutschen Text (oder einem monoalphabetisch verschlüsselten deutschen Text) wird dieser Wert mit hoher Wahrscheinlichkeit größer als 6 % sein.
Bestimmen Sie den $\widetilde{IC}$-Wert von PANAMAKANAL und von TEPRYMEXQFY (durch einen Zufallsgenerator zustande gekommen).

12.) Verschlüsseln Sie mit Hilfe der Playfair-Chiffre und des Schlüssels KRYPTO den Klartext MORGENINALLERFRUEHDIEBURGANGREIFEN.
Verwenden Sie denselben Schlüssel und Klartext und stattdessen die Vigenère-Chiffre.

13.) Ein Kryptoanalytiker versucht, eine Vigenère-verschlüsselte Chiffre zu knacken. Ihm fallen folgende Buchstabenwiederholungen im Text auf:

$$\dots.\text{XSD}\dots\text{AWER}\dots\dots\text{XSD}\dots\dots\dots\text{AWER}\dots$$

Welche Vermutung über die verwendete Schlüsselwortlänge stellt er auf?

14.) Wir führen 2 Zufallsexperimente durch:
Beim ersten Experiment wählen wir unter Gleichverteilung aus der Menge der 26 Buchstaben (mit Zurücklegen) n-mal aus. Sei X die Zufallsvariable, die die Anzahl der "Kollisionen" zählt; dies ist die Anzahl der (i,j) mit $1 \leq i < j \leq n$, so dass der i-te und der j-te Buchstabe identisch sind.
Beim zweiten Experiment wird ein zufällig ausgewählter deutscher Text der Länge n gewählt. Man kann davon ausgehen, dass ein deutscher Text den Koinzidenzindex von 7 Prozent hat.
Definition von Koinzidenzindex: $IC = \sum_{i=1}^{26} (p_i)^2$, wobei p_i die Auftretenswahrscheinlichkeit des i-ten Buchstaben ist. (Beispiel: der Buchstabe E tritt im Deutschen am häufigsten auf; nämlich mit Wahrscheinlichkeit ca. 17 Prozent.)
Berechnen Sie den Erwartungswert von X in beiden Experimenten. Bei wievielen Buchstaben wird im ersten (bzw. im zweiten) Experiment der Wert $E(X) = 1$ gerade überschritten?

15.) Verschlüsseln Sie den Text RUNDERHUNDINDEX mit Vigenère-Verschlüsselung. Verwenden Sie dazu das Schlüsselwort BAD.

Wenden Sie die Kasiski-Methode an, um die Schlüsselwortlänge zu ermitteln.

16.) Geben Sie eine homophone Chiffrierung mit den Ziffern von 0 bis 9 als Chiffrealphabet an, die an ein Klartextalphabet aus den Buchstaben A, B, C, D angepasst ist, welche jeweils mit den Wahrscheinlichkeiten $0.2, 0.4, 0.1, 0.3$ auftreten.

17.) Nehmen Sie an, die Buchstaben A, B, C, D treten mit den in Aufgabe 16 angegebenen Wahrscheinlichkeiten auf. Berechnen Sie die Shannon-Entropie, den Koinzidenzindex und die Renyi-Entropie (Taschenrechner!).

18.) Der beste bekannte Algorithmus, um ein bestimmtes kryptographisches System XYZ mit der Schlüsselwortlänge n zu knacken, habe Laufzeit $2^{n/7}$. Wenn man davon ausgeht, dass ein 80 Bit langer Schlüssel gegenüber einem Brute-Force-Angriff ein ausreichendes Sicherheitsniveau besitzt, wie lang sollten die Schlüssel beim XYZ-Verfahren sein, um ein ähnliches, ausreichendes Sicherheitsniveau zu erreichen?

19.) Die Pop-Gruppe *The Repetitives* setzt ihre Songs aus folgenden Bestandteilen zusammen, die mit folgenden relativen Häufigkeiten auftreten:

UHU	1/8
AHA	1/2
YEAH	1/4
BABY	1/8

Berechnen Sie den Koinzidenzindex und die Entropie dieser Wahrscheinlichkeitsverteilung.

20.) In Krüptöpia verwendet man (wegen der vielen Umlaute) ein Alphabet mit 30 Buchstaben. Was Chiffrieren betrifft, so ist man allerdings noch rückständig (oder zu gutgläubig): Es wird eine monoalphabetische affine Chiffre verwendet. Wie viele verschiedene Schlüssel stehen dabei zur Verfügung? Wie viele Schlüssel wären es, wenn man etwas sparsamer wäre und mit 29 Buchstaben auskäme?

21.) Beim Zwergen-Lotto werden von 7 Feldern genau 3 zufällig angekreuzt. Bestimmen Sie die Shannon-Entropie dieses Zufallsexperiments (Taschenrechner).

22.) Wenn wir davon ausgehen, dass ein Schlüsselwort bei der Playfair-Chiffre die Länge 5 haben soll, wobei die 5 Buchstaben voneinander verschieden sein müssen, wieviele Schlüssel gibt es dann? Was macht das gemessen als Bitlänge? Wenn das Schlüsselwort ein deutsches Wort sein soll, wobei wir von einer Entropie von 2 bit pro Buchstabe ausgehen, welche Bitlänge erhalten wir dann?