Wiederholung / Fragen zur letzten Vorlesung

- Der Operator „mod" kommt in der Vorlesung auf 2 Arten vor:

  $x \bmod k$ ... Rest bei der Division von x durch k, eine Zahl zwischen 0 und $k-1$. (Programmiersprachen-Konstrukt)

  bzw: $x \equiv y \pmod k$ (mathematisches Konstrukt)

  Sprich: x ist kongruent y, modulo k

  bedeutet: $x-y$ ist durch k teilbar. (ein Vielfaches von k)

  Es gilt:

  $x \equiv y \pmod k$ gdw. $x \bmod k = y \bmod k$

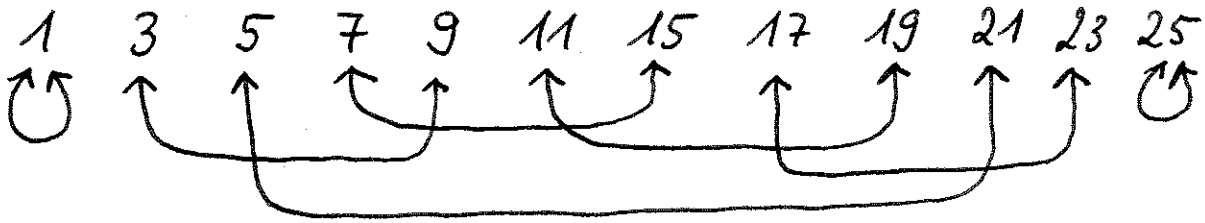
Frage: In der Vorlesung wurde gesagt, dass die Zahl 26 genau $\varphi(26) = 12$ teilerfremde nat. Zahlen < 26 besitzt. (a, b teilerfremd $\Leftrightarrow$ $ggT(a,b) = 1$).
Man gebe diese Zahlen explizit an!

Antwort:

$$\Pi_{26}^{*} = \{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\}$$

Aufgabe: Man finde für jede Zahl in $\mathbb{Z}_{26}^*$ sein multiplikatives Inverses. (Also, zu $x \in \mathbb{Z}_{26}^*$ dasjenige y mit $x \cdot y \equiv 1 \pmod{26}$.)

Antwort:



Frage: Gegeben sei die affine Chiffrierung

$$c = E(a, (3,4)) = (3 \cdot a + 4) \bmod 26$$

Auch die Dechiffrierung $a = D(c, (k_1, k_2)) = (k_1 \cdot a + k_2) \bmod 26$ kann als affine Funktion beschrieben werden. Man bestimme k_1 und k_2!

Antwort: Es gilt:

$$c \equiv 3a + 4 \pmod{26}$$

$$\text{gdw. } c - 4 \equiv 3a \pmod{26}$$

$$\text{gdw. } 9 \cdot (c-4) \equiv a \pmod{26}$$

$$\text{gdw. } a \equiv 9c - 36 \pmod{26}$$

$$\text{gdw. } a \equiv 9c - 10 \pmod{26}$$

$$\text{gdw. } a \equiv \underbrace{9}_{k_1} c + \underbrace{16}_{k_2} \pmod{26}$$

Aufgabe: Entschlüssele (ohne Kenntnis des Schlüssels) folgende monoalphabetische Chiffre:

WE JWEFZWZWR RMFZ IWXFZWR TRA NTRAWB

ES GESCHEHEN NOCH ZEICHEN UND WUNDER

Auszählen der Buchstaben ergibt folgende Häufigkeiten:

W...7, R...5, Z...4, F...3, T...2, die restlichen ...1-mal
E...2

Die häufigsten Buchstaben im Deutschen sind:

E, N, I, R, S, A, T, ...

Die häufigsten Buchstabenpaare (Bigramme) sind:

ER, EN, CH, DE, EI, ND, TE, IN, IE, GE, ES, NE

Die häufigsten Buchstaben-Tripel (Trigramme) sind:

EIN, ICH, NDE, DIE, UND, DER, CHE, END, GEN, SCH

Aufgabe: Eine Schlüssellänge von ≥80 Bit ist dann ausreichend lang, wenn die einzige Form der Kryptoanalyse darin besteht, alle Schlüssel („brute-force") auszuprobieren. Nimmt man an, die schnellsten Computer – mit massiver Parallelität – können einen Schlüssel in der Zeit 10^{-12} sec analysieren. Wie lange braucht man dann?

Antwort: $2^{80} \cdot 10^{-12}$ sec $\approx$ 38 000 Jahre

Bemerkung: Diese Zahl $n = 80$ Bit kommt in der Vorlesung öfters vor. Angenommen, um eine Zahl n ($= p \cdot q$) in ihre Primfaktoren zu faktorisieren, benötigt der schnellste bekannte Algorithmus etwa $2^{m/12}$ Rechenschritte (m = Anzahl Bits der Zahl n)

Um das notwendige Sicherheitsniveau von 80 Bit zu erreichen, sollte n also eine Zahl mit $m = 12 \cdot 80 \approx 1000$ Bits sein.

Definition: Ein Krypto-Verfahren hat ein Sicherheitsniveau von k Bits, wenn der schnellste bekannte Algorithmus zum Knacken des Kryptosystems Laufzeit 2^k hat.
(Daraus lässt sich dann, wie beim obigen Beispiel, die notwendige Schlüssellänge berechnen.)

Frage: Was ist ein monoalphabetisches Kryptoverfahren – im Unterschied zu einem polyalphabetischen?

Antwort: Jeder Einzelbuchstabe des Klartexts wird auf einen festen Buchstaben der Chiffre abgebildet. Die Art der Abbildung wird durch den Schlüssel gesteuert.
Bei polyalphabetischer Verschlüsselung kann aus demselben Klartextbuchstaben jedesmal ein anderer Chiffrebuchst. entstehen.

---

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
09	78	48	13	45	25	39	65	83	51	84	22	58	71	95	29	35	40	76	49	61	89	28	21	52	66
12	92	81	41	79	23	50	68	88			27	59	91	94			42	86	69	63					
33			62	14		56	32	93			18		00				77	96	75	34					
47			01	16			70	15					05				80	17	85	60					
53			03	24			73	04					07				11	20	97						
67				44				26					54				19	30	08						
				46				37					72				36	43							
				55				58					90												
				57									99												
				64									38												
				74																					
				82																					
				87																					
				98																					
				10																					
				31																					
				06																					

Beispiel für eine homophone Verschlüsselung.

$C : \{A, B, \ldots, Z\} \to \{00, 01, 02, \ldots, 98, 99\}$ stochastische Abbildung.

Erzeugt eine Gleichverteilung auf $\{00, \ldots, 99\}$ auf Einzelbuchstaben.

Bigramme/Trigramme nach wie vor „verräterisch".

Die Verteilung der Buchstaben im Deutschen weicht stark von einer Gleichverteilung ab. Sei

$$P = (p_1, p_2, \dots, p_n) \; ; \quad \sum_{i=1}^{n} p_i = 1 \; ; \quad n = 26$$

die Verteilung der Buchstaben im Deutschen.

Koinzidenzindex: $IC(P) := \sum_{i=1}^{n} p_i^2$

- Gleichverteilung: $IC(P) = \frac{1}{n}$
- $IC(P) = 1$ bei determ. Verteilg.

Für die deutsche Sprache gilt: $IC(P) \approx 0{,}07$

Bei Gleichverteilung $p_i = \frac{1}{26}$ bei $n = 26$ gilt

dagegen: $IC(P) = 0{,}0385 = \frac{1}{26}$.

Interpretation von $IC(P)$: Dies ist die Wahrscheinlichkeit, dass bei 2 zufällig ausgewählten Buchstaben diese identisch sind. Seien X und Y Zufallsvariablen, beide unabhängig und gemäß P verteilt. Dann ist $IC(P) = P(X = Y)$.

- $-\log_2 IC(P)$ nennt man Renyi-Entropie

Frage: Sei T ein (langer) Text und $R = (r_1, r_2, \dots, r_{26})$ die relative Häufigkeit der einzelnen Buchstaben im Text T (als Schätzung für die zugrunde liegende Wahrscheinlichkeitsverteilung).

Wenn T eine monoalphabetische Chiffre ist (z.B. durch Cäsar oder affin entstanden), welchen Wert $IC(r_1,\dots,r_{26})$ erhalten wir etwa?

Antwort: Ca. ~~3,85%~~ 7%

Gegeben seien 2 Wahrscheinlichkeits/Häufigkeitsverteilungen

$P = (p_1,\dots,p_{26})$ $\quad$ $Q = (q_1,\dots,q_{26})$

z.B. Verteilung im Deutschen

z.B. Häufigkeits-verteilung eines Textes.

Maß für die Ähnlichkeit von P und Q ist:

paarweiser Koinzidenzindex: $IC(P,Q) = \sum_{i=1}^{26} p_i \cdot q_i$

wird maximal (ca 7%) bei Übereinstimmung

Eine mögliche Anwendung: Gegeben ist ein chiffrierter Text T (mittels affiner Chiffre). Es gibt 312 verschiedene Schlüssel (k_1,k_2). Man wendet auf T (per Computer) diese 312 Schlüssel an und vergleicht das Ergebnis mit Verteilung der deutschen

Sprache. Beim richtigen Schlüssel springt der Wert $IC(P,Q)$ hoch auf ca 7% (sonst: $\leq 4\%$)

Playfair-Chiffre (bi-alphabetisch)

Durch einen Schlüssel gesteuerte Abbildung

$$\{A,B,\dots,Z\}^2 \longrightarrow \{A,B,\dots,Z\}^2$$

Einschränkung: I=J, also nur $25 = 5 \cdot 5$ Buchstaben.

Weitere Einschränkung: Kein Buchstaben-Paar darf aus 2 gleichen Buchstaben bestehen.

Schlüsselwort, z.B. DEATH, in 1. Zeile eintragen in ein 5×5 Schema. Dieses mit den restlichen Buchstaben des Alphabets auffüllen:

Buchst. in derselben Zeile/Spalte zykl. Shift um 1 Pos. nach rechts/unten

D	E	A	T	H
B	C	F	G	I
K	L	M	N	O
P	Q	R	S	U
V	W	X	Y	Z

Buchst. bilden Ecken eines Rechtecks: im Uhrzeigersinn verdrehen.

Klartext: MO|RG|EN|FR|UE|HA|NG|RE|IF|EN

Chiffre: NK FS TL MX QH DT SN QA BG TL

VIGENÈRE-Chiffre

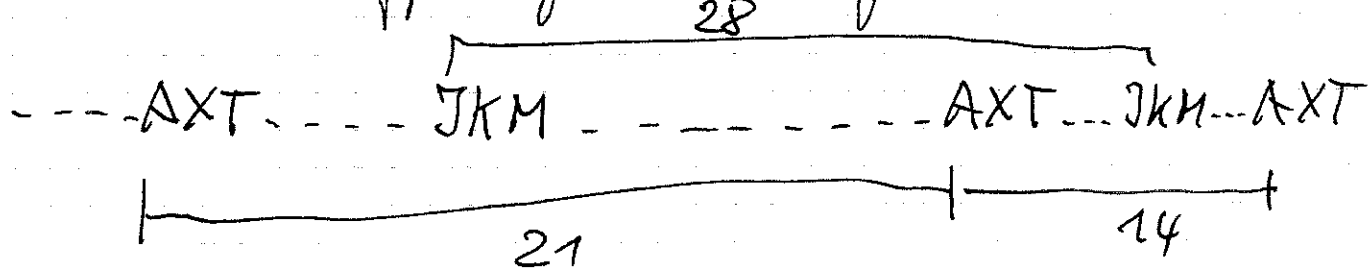
galt über Jahrhunderte als nicht-knackbar (bis ca. 1850)

Das Schlüsselwort (hier: DEATH) wiederholt unter den Klartext schreiben und modulo 26 addieren (ohne Übertrag):

```
  M O R G E N F R U E H A N G R E I F E N
+ D E A T H D E A T H D E A T H D E A T H
-----------------------------------------
  P S R Z L Q J R N L K E N Z Y H M F X U
```

Dechiffrieren nach Kasiski-Methode

Finde in Chiffre gleiche Trigramme



$ggT(21, 28, 14) = 7$ ... vermutete Schlüsselwortlänge