Hilly – Eine verbesserte Hill-Chiffre

Yahya Almardeny und Anna Lena Rotthaler

Version 1.0 – 23.01.17

Inhaltsverzeichnis

Diese Challenge stellt eine verbesserte Version der Hill-Chiffre dar. Die Verbesserung besteht aus einer dynamischen Substitutionstabelle (Schritt 2 und 3)(berechnet aus den Diagonalelementen der Schlüsselmatrix), und einer Erweiterung, den sog. „Extensions“ (Schritte 9 bis 14).
Im Gegensatz zur klassischen Hill-Chiffre soll die Schlüsselmatrix hier nur „invertierbar“ sein, aber nicht invertierbar modulo 26. Die Determinante der Schlüsselmatrix darf daher nicht die Werte 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25 mod 26 annehmen. D.h. für sie muss gelten: gcd(det(K),26) $\neq 1$. Positiv ausgedrückt darf die Determinante nur einen der folgenden Werte mod 26 haben: 2, 4, 6, 8, 10, 12, 13, 14, 16, 18, 20, 22, 24.

1 Verschlüsselung

1. Wählen Sie eine invertierbare $n * n$-Matrix K als Schlüssel mit $n \geq 5$ und $n = 6$ als Default, wobei für K gelten muss: gcd(det(K), 26) $\neq 1$.

2. Berechnen Sie s wie folgt: Summieren Sie die Elemente der Hauptdiagonalen von K (die Hauptdiagonale geht von links oben nach rechts unten).
   Falls s=0: Summieren Sie die Elemente der Nebendiagonalen von K (die Nebendiagonale geht von rechts oben nach links unten).
   Falls auch dieses s=0: Generieren Sie eine neue Schlüsselmatrix.

3. Berechnen Sie die Substitutionstabelle T_P für das Klartextzeichen-Alphabet:
   A=s, B=(2*s), C=(3*s), D=(4*s), ... , Z=(26*s)

4. Teilen Sie den Klartext in Blöcke von n Zeichen ein.
   Bitte achten Sie darauf, dass die Klartext-Länge einem Vielfachen von n entspricht (siehe Bemerkung 3.4).

5. Ersetzen Sie die Klartext-Buchstaben durch Zahlen mit Hilfe der Substitutionstabelle T_P. Sie erhalten den Klartext-Zahlenvektor P.

6. Multiplizieren Sie K mit P, um den Vektor C1 zu erhalten: C1 = K * P

7. Berechnen Sie den Geheimtext-Vektor C = C1 mod 26.

8. Substituieren Sie die Elemente in C mit Hilfe der Substitutionstabelle T_C für das Geheimtext-Alphabet: 0=Z, 1=A, 2=B, ..., 24=X, 25=Y.

9. Berechnen Sie den „Extension-Vektor“ X wie folgt: Teilen Sie C1 durch 26 und runden Sie die Werte auf: X = Upperbound (C1 / 26)

10. Die „Extension-Matrix“ E ergibt sich, indem Sie den Wert s zu jedem Element von K addieren: E = s * I + K (I ist die Eins-Matrix)

11. Berechnen Sie die „verschlüsselten Extensions“ X_{Enc}, indem Sie E mit X multiplizieren: $X_{Enc} = E * X$

12. Verbinden Sie alle Geheimtext-Buchstaben mit ihren verschlüsselten Extensions: $C_1\ X_{Enc1}\ \ldots\ C_6\ X_{Enc6}$

13. Legen Sie 11 zusätzliche Symbole (eines für jede der 10 Dezimalziffern und eines für das Minus-Zeichen) fest: (*, #, &, %, $, +, ?, !, @, ^, -). Erstellen Sie dann eine Substitutionstabelle T_A für diese Symbole wie folgt:
    a) Berechnen Sie die Summe t aller Elemente der Schlüsselmatrix mod 11.
    b) Falls t Null ist, sieht die Substitutionstabelle T_A für zusätzliche Symbole wie folgt aus:

-	0	1	2	3	4	5	6	7	8	9
*	#	&	%	$	+	?	!	@	^	-

       Ansonsten verschieben Sie die Symbole um das Ergebnis aus Schritt (a) nach rechts.

14. Substituieren Sie X_{Enc} mit der Substitutionstabelle T_A. Sie erhalten X_{EncSym}.

15. Senden Sie ($C_1\ X_{EncSym1}\ \ldots\ C_6\ X_{EncSym6}$) an den Empfänger.

1.1 Beispiel

Gegeben: Klartext ABCDEF

1. $K = \begin{pmatrix} 4 & 3 & 6 & 6 & 2 & 3 \\ 7 & 4 & 2 & 1 & 5 & 1 \\ 2 & 5 & 7 & 8 & 3 & 8 \\ 8 & 3 & 4 & 4 & 9 & 7 \\ 5 & 1 & 1 & 1 & 4 & 5 \\ 0 & 9 & 8 & 9 & 8 & 8 \end{pmatrix}$
2. $s = 31$
3. Substitutionstabelle T_P für das Klartextzeichen-Alphabet:
   A=31, B=62, C=93, D=124, E=155, F=186
4. P: ABCDEF
5. $P = \begin{pmatrix} 31 \\ 62 \\ 93 \\ 124 \\ 155 \\ 186 \end{pmatrix}$
6. $C1 = K * P = \begin{pmatrix} 4 & 3 & 6 & 6 & 2 & 3 \\ 7 & 4 & 2 & 1 & 5 & 1 \\ 2 & 5 & 7 & 8 & 3 & 8 \\ 8 & 3 & 4 & 4 & 9 & 7 \\ 5 & 1 & 1 & 1 & 4 & 5 \\ 0 & 9 & 8 & 9 & 8 & 8 \end{pmatrix} * \begin{pmatrix} 31 \\ 62 \\ 93 \\ 124 \\ 155 \\ 186 \end{pmatrix} = \begin{pmatrix} 2480 \\ 1736 \\ 3968 \\ 3999 \\ 1984 \\ 5146 \end{pmatrix}$
7. $C = C1 \bmod 26 = \begin{pmatrix} 2480 \\ 1736 \\ 3968 \\ 3999 \\ 1984 \\ 5146 \end{pmatrix} \bmod 26 = \begin{pmatrix} 10 \\ 20 \\ 16 \\ 21 \\ 8 \\ 24 \end{pmatrix}$
8. $C = \begin{pmatrix} J \\ T \\ P \\ U \\ H \\ X \end{pmatrix}$
9. $X = \text{Upperbound } (C1 \,/\, 26) = \lceil \begin{pmatrix} 2480 \\ 1736 \\ 3968 \\ 3999 \\ 1984 \\ 5146 \end{pmatrix} : 26 \rceil = \lceil \begin{pmatrix} 95,38 \\ 66,76 \\ 152,61 \\ 153,80 \\ 76,30 \\ 197,92 \end{pmatrix} \rceil = \begin{pmatrix} 96 \\ 67 \\ 153 \\ 154 \\ 77 \\ 198 \end{pmatrix}$

10. $E = s * I + K = \begin{pmatrix} 31 & 31 & 31 & 31 & 31 & 31 \\ 31 & 31 & 31 & 31 & 31 & 31 \\ 31 & 31 & 31 & 31 & 31 & 31 \\ 31 & 31 & 31 & 31 & 31 & 31 \\ 31 & 31 & 31 & 31 & 31 & 31 \\ 31 & 31 & 31 & 31 & 31 & 31 \end{pmatrix} + \begin{pmatrix} 4 & 3 & 6 & 6 & 2 & 3 \\ 7 & 4 & 2 & 1 & 5 & 1 \\ 2 & 5 & 7 & 8 & 3 & 8 \\ 8 & 3 & 4 & 4 & 9 & 7 \\ 5 & 1 & 1 & 1 & 4 & 5 \\ 0 & 9 & 8 & 9 & 8 & 8 \end{pmatrix} = \begin{pmatrix} 35 & 34 & 37 & 37 & 33 & 34 \\ 38 & 35 & 33 & 32 & 36 & 32 \\ 33 & 36 & 38 & 39 & 34 & 39 \\ 39 & 34 & 35 & 35 & 40 & 38 \\ 36 & 32 & 32 & 32 & 35 & 36 \\ 31 & 40 & 39 & 40 & 39 & 39 \end{pmatrix}$

11. $X_{Enc} = E * X = \begin{pmatrix} 35 & 34 & 37 & 37 & 33 & 34 \\ 38 & 35 & 33 & 32 & 36 & 32 \\ 33 & 36 & 38 & 39 & 34 & 39 \\ 39 & 34 & 35 & 35 & 40 & 38 \\ 36 & 32 & 32 & 32 & 35 & 36 \\ 31 & 40 & 39 & 40 & 39 & 39 \end{pmatrix} * \begin{pmatrix} 96 \\ 67 \\ 153 \\ 154 \\ 77 \\ 198 \end{pmatrix} = \begin{pmatrix} 26270 \\ 25078 \\ 27740 \\ 27371 \\ 25247 \\ 28508 \end{pmatrix}$

12. Konkatenation: $\begin{pmatrix} \text{J26270} \\ \text{T25078} \\ \text{P27740} \\ \text{U27371} \\ \text{H25247} \\ \text{X28508} \end{pmatrix}$

13. a) 171 mod 11 = 6

    b)

-	0	1	2	3	4	5	6	7	8	9
+	?	!	@	^	-	*	#	&	%	$

14. (C, X_{EncSym}) = J@#@&?T@*?&%P@&&-?U@&^&!H@*@-&X@%*?%

15. Das Ergebnis des letzten Schritts als Geheimtext versenden.

2 Entschlüsselung

Gegeben: der Geheimtext in der Form (C_1 $X_{EncSym1}$ ... C_6 $X_{EncSym6}$) und die Schlüsselmatrix K.

1. Berechnen Sie die Diagonalsumme s aus der Schlüsselmatrix K und dann daraus die entsprechende Substitutionstabelle T_P für das Klartextzeichen-Alphabet.

2. Berechnen Sie die Summe aller Elemente von K mod 11 und die daraus resultierende Substitutionstabelle T_A für zusätzliche Symbole.
   Resubstituieren Sie die Geheimtext-Zeichen X_{EncSym} mit Hilfe der Substitutionstabelle T_A, um die „Verschlüsselten Extensions“ X_{Enc} herauszufinden.

3. Substituieren Sie alle Geheimtext-Buchstaben aus C mit Hilfe der Substitutionstabelle T_C: A=1, B=2,..., Z=26.

4. Die „Extension-Matrix“ E ergibt sich, indem Sie den Wert s zu jedem Element von K addieren: E = s * I + K (I ist die Eins-Matrix)

5. Berechnen Sie die Inverse K^{-1} von K und die Inverse E^{-1} von E.

6. Multiplizieren Sie E^{-1} mit X_{Enc}, um den „Extension-Vektor“ X zu erhalten: $X = E^{-1} * X_{Enc}$

7. Benutzen Sie die folgende Formel, um C1 zu berechnen (C1 war das Ergebnis der Multiplikation der Schlüsselmatrix K mit dem substituierten Klartext): C1 = (X * 26) - (26 - C).

8. Multiplizieren Sie K^{-1} mit C1 (wenn Sie mit den exakten Brüchen rechnen, ist Runden nicht erforderlich): $P = K^{-1} * C1$

9. Substituieren Sie P mit der Substitutionstabelle T_P.

2.1 Beispiel

Gegeben: Geheimtext J@#@&?T@*?&%P@&&-?U@&^&!H@*@-&X@%*?% und Schlüssel K

$$K = \begin{pmatrix} 4 & 3 & 6 & 6 & 2 & 3 \\ 7 & 4 & 2 & 1 & 5 & 1 \\ 2 & 5 & 7 & 8 & 3 & 8 \\ 8 & 3 & 4 & 4 & 9 & 7 \\ 5 & 1 & 1 & 1 & 4 & 5 \\ 0 & 9 & 8 & 9 & 8 & 8 \end{pmatrix}$$

1. s=31; A=31, B=62, C=93, D=124, E=155, F=186

2. 171 mod 11 = 6 →

-	0	1	2	3	4	5	6	7	8	9
+	?	!	@	^	-	*	#	&	%	$

$$X_{Enc} = \begin{pmatrix} 26270 \\ 25078 \\ 27740 \\ 27371 \\ 25247 \\ 28508 \end{pmatrix}$$

3. $C = \begin{pmatrix} 10 \\ 20 \\ 16 \\ 21 \\ 8 \\ 24 \end{pmatrix}$

4. $E = s * I + K = \begin{pmatrix} 31 & 31 & 31 & 31 & 31 & 31 \\ 31 & 31 & 31 & 31 & 31 & 31 \\ 31 & 31 & 31 & 31 & 31 & 31 \\ 31 & 31 & 31 & 31 & 31 & 31 \\ 31 & 31 & 31 & 31 & 31 & 31 \\ 31 & 31 & 31 & 31 & 31 & 31 \end{pmatrix} + \begin{pmatrix} 4 & 3 & 6 & 6 & 2 & 3 \\ 7 & 4 & 2 & 1 & 5 & 1 \\ 2 & 5 & 7 & 8 & 3 & 8 \\ 8 & 3 & 4 & 4 & 9 & 7 \\ 5 & 1 & 1 & 1 & 4 & 5 \\ 0 & 9 & 8 & 9 & 8 & 8 \end{pmatrix} = \begin{pmatrix} 35 & 34 & 37 & 37 & 33 & 34 \\ 38 & 35 & 33 & 32 & 36 & 32 \\ 33 & 36 & 38 & 39 & 34 & 39 \\ 39 & 34 & 35 & 35 & 40 & 38 \\ 36 & 32 & 32 & 32 & 35 & 36 \\ 31 & 40 & 39 & 40 & 39 & 39 \end{pmatrix}$

5. $K^{-1} = \begin{pmatrix} \frac{-128}{163} & \frac{71}{163} & \frac{164}{163} & \frac{105}{163} & \frac{-198}{163} & \frac{-93}{163} \\ \frac{-100}{163} & \frac{283}{652} & \frac{431}{652} & \frac{26}{163} & \frac{-415}{652} & \frac{-37}{163} \\ \frac{1031}{163} & \frac{-1661}{652} & \frac{-4693}{652} & \frac{-819}{163} & \frac{6145}{652} & \frac{595}{163} \\ \frac{-932}{163} & \frac{1477}{652} & \frac{4369}{652} & \frac{790}{163} & \frac{-5889}{652} & \frac{-560}{163} \\ \frac{9}{163} & \frac{-19}{163} & \frac{-37}{163} & \frac{27}{163} & \frac{-9}{163} & \frac{18}{163} \\ \frac{121}{163} & \frac{-243}{652} & \frac{-559}{652} & \frac{-126}{163} & \frac{983}{652} & \frac{79}{163} \end{pmatrix}$

$E^{-1} = \begin{pmatrix} \frac{-965}{1248} & \frac{49}{78} & \frac{733}{624} & \frac{283}{416} & \frac{-1531}{1248} & \frac{-341}{6243} \\ \frac{-3035}{4992} & \frac{163}{312} & \frac{1843}{2496} & \frac{293}{1664} & \frac{-3205}{4992} & \frac{-539}{2496} \\ \frac{31001}{4992} & \frac{-1369}{312} & \frac{-21985}{2496} & \frac{-8935}{1664} & \frac{47623}{4992} & \frac{8537}{2496} \\ \frac{-28001}{4992} & \frac{1249}{312} & \frac{20521}{2496} & \frac{8607}{1664} & \frac{-45631}{4992} & \frac{-8033}{2496} \\ \frac{71}{1248} & \frac{-7}{78} & \frac{-127}{624} & \frac{71}{416} & \frac{-71}{1248} & \frac{71}{624} \\ \frac{1205}{1664} & \frac{-69}{104} & \frac{-925}{832} & \frac{-1377}{1664} & \frac{2539}{1664} & \frac{373}{832} \end{pmatrix}$

6. $X = E^{-1} * X_{Enc} = \begin{pmatrix} \frac{-965}{1248} & \frac{49}{78} & \frac{733}{624} & \frac{283}{416} & \frac{-1531}{1248} & \frac{-341}{6243} \\ \frac{-3035}{4992} & \frac{163}{312} & \frac{1843}{2496} & \frac{293}{1664} & \frac{-3205}{4992} & \frac{-539}{2496} \\ \frac{31001}{4992} & \frac{-1369}{312} & \frac{-21985}{2496} & \frac{-8935}{1664} & \frac{47623}{4992} & \frac{8537}{2496} \\ \frac{-28001}{4992} & \frac{1249}{312} & \frac{20521}{2496} & \frac{8607}{1664} & \frac{-45631}{4992} & \frac{-8033}{2496} \\ \frac{71}{1248} & \frac{-7}{78} & \frac{-127}{624} & \frac{71}{416} & \frac{-71}{1248} & \frac{71}{624} \\ \frac{1205}{1664} & \frac{-69}{104} & \frac{-925}{832} & \frac{-1377}{1664} & \frac{2539}{1664} & \frac{373}{832} \end{pmatrix} * \begin{pmatrix} 26270 \\ 25078 \\ 27740 \\ 27371 \\ 25247 \\ 28508 \end{pmatrix} = \begin{pmatrix} 96 \\ 67 \\ 153 \\ 154 \\ 77 \\ 198 \end{pmatrix}$

7. $C1 = (X * 26) - (26 - C) = (\begin{pmatrix} 96 \\ 67 \\ 153 \\ 154 \\ 77 \\ 198 \end{pmatrix} * 26) - (26 - \begin{pmatrix} 10 \\ 20 \\ 16 \\ 21 \\ 8 \\ 24 \end{pmatrix}) = \begin{pmatrix} 2480 \\ 1736 \\ 3968 \\ 3999 \\ 1984 \\ 5146 \end{pmatrix}$

8. $P = K^{-1} * C1 = \begin{pmatrix} \frac{-128}{163} & \frac{71}{163} & \frac{164}{163} & \frac{105}{163} & \frac{-198}{163} & \frac{-93}{163} \\ \frac{-100}{163} & \frac{283}{652} & \frac{431}{652} & \frac{26}{163} & \frac{-415}{652} & \frac{-37}{163} \\ \frac{1031}{163} & \frac{-1661}{652} & \frac{-4693}{652} & \frac{-819}{163} & \frac{6145}{652} & \frac{595}{163} \\ \frac{-932}{163} & \frac{1477}{652} & \frac{4369}{652} & \frac{790}{163} & \frac{-5889}{652} & \frac{-560}{163} \\ \frac{9}{163} & \frac{-19}{163} & \frac{-37}{163} & \frac{27}{163} & \frac{-9}{163} & \frac{18}{163} \\ \frac{121}{163} & \frac{-243}{652} & \frac{-559}{652} & \frac{-126}{163} & \frac{983}{652} & \frac{79}{163} \end{pmatrix} * \begin{pmatrix} 2480 \\ 1736 \\ 3968 \\ 3999 \\ 1984 \\ 5146 \end{pmatrix} = \begin{pmatrix} 31 \\ 62 \\ 93 \\ 124 \\ 155 \\ 186 \end{pmatrix}$

9. $P = \begin{pmatrix} 31 \\ 62 \\ 93 \\ 124 \\ 155 \\ 186 \end{pmatrix} = \begin{pmatrix} A \\ B \\ C \\ D \\ E \\ F \end{pmatrix}$

3 Bemerkungen

3.1 Zur Substitutionstabelle T_P für das Klartext-Alphabet

Klartext- und Geheimtext-Alphabet enthalten – wie beim normalen Hillverfahren – jeweils die 26 Großbuchstaben. s wird definiert in Schritt 2.

- Aufgrund von s sind Klartextbuchstaben keinem festen Zahlenwert mehr zugeordnet, sondern Vielfachen von s.
- Es gibt zwei verschiedene Substitutionstabellen – eine für das Klartextalphabet T_P und eine für das Geheimtextalphabet T_C.
  Die Zahlenwerte, die darin den Buchstaben zugeordnet werden, sind unterschiedlich:
  - T_P=(A=s, B=2*s, ..., Z=26*s) und
  - T_C=(0=Z, 1=A, 2=B, ..., 25=Y) [Verschlüsselung] bzw.
    T_C=(1=A, 2=B, ... , Z=26) [Entschlüsselung].

3.2 Zur Substitutionstabelle T_C für das Geheimtext-Alphabet

Die Substitutionstabelle T_C unterscheidet sich bei der Verschlüsselung (Schritt 8) und bei der Entschlüsselung (Schritt 3). Bei der Verschlüsselung ist Z=0 und bei der Entschlüsselung ist Z=26.
Das liegt daran, dass bei der Verschlüsselung X = Upperbound (C1 / 26) berechnet wird. Um diese Rundung rückgängig zu machen, muss bei der Entschlüsselung (26-C) abgezogen werden. Ist bei der Verschlüsselung C=0, so ist C1 ein Vielfaches von 26 und damit erfolgt keine Rundung bei der Berechnung von X. In diesem Fall muss auch bei der Entschlüsselung für C=0 gelten: (26-C) = 0, da keine Rundung ausgeglichen werden muss und daher muss C hier gleich 26 sein.

3.3 Zur Substitutionstabelle T_A für zusätzliche Symbole

Die Substitutionstabelle T_A besteht aus 11 Symbolen, eines für jede der zehn Dezimalziffern und eines für das Minus-Zeichen.
Der Geheimtext im obigen Beispiel in dieser Beschreibung enthält kein dem Minus-Zeichen entsprechendes Zeichen (hier wäre es das + Zeichen), da die Werte der Schlüsselmatrix alle positiv sind.
Wenn negative Werte in der Schlüsselmatrix enthalten sind, können daraus negative Encrypted Extensions resultieren und dann tritt das Minus-Zeichen auch im Geheimtext auf. Daher muss es auch in der Substitutionstabelle T_A enthalten sein, da ein Angreifer ansonsten Informationen über die Schlüsselmatrix bekommen würde.

3.4 Padding

3.4.1 Verschlüsselung

Falls die Klartext-Länge nicht ein Vielfaches von n beträgt und man es dem Benutzer nicht aufbürden will, seinen Klartext aufzufüllen, ist Padding erforderlich.

Unter den oben gemachten Voraussetzungen (die Klartext-Länge ist ein Vielfaches von n) jedoch ist kein Padding erforderlich.

Im Folgenden ist ein Beispiel für ein händisches Verfahren beschrieben, das bis zu einer Größe von n=6 funktioniert. (Dazu wird eine weitere Tabelle T_S eingeführt: Bei einer Blocklänge von n braucht man genau n weitere Symbole, die weder im Klartextalphabet noch in T_A vorkommen dürfen. Wenn man sehr große Matrizen verwendet, würden einem also die Symbole ausgehen.)

Aufgefüllt werden soll mit dem letzten Buchstaben des Klartextes, bis die Länge ein Vielfaches von n

ergibt. (Beispiel: n = 6, BEISPIEL → BEISPIELLLLL)

Um kenntlich zu machen, ob Padding verwendet wurde, soll Folgendes gemacht werden:

1. Berechnen Sie R = n - (Anzahl der Buchstaben des Klartextes mod n).
   (Beispiel: R = 6 - (8 mod 6) = 6 - 2 = 4.)

2. Falls R = n, ändern Sie es in R = 0 (kein Padding).

3. Substituieren Sie R mit Hilfe der folgenden Tabelle T_S für Symbole:

0	1	2	3	4	5
”	\	:	;	,	.

   Hängen Sie das Symbol an den Geheimtext an.
   (Beispiel: Das Symbol in T_S für 4 ist “ , ”. BEISPIELLLLL → BEISPIELLLLL,)

3.4.2 Entschlüsselung

Da das letzte Zeichen des Geheimtextes das Zeichen für R ist, müssen dieses Zeichen und die entsprechenden R Zeichen des entschlüsselten Texts vor R entfernt werden, um den Klartext zu erhalten.

3.5 Substitutionstabellen in Hill und Hilly

Das Hilly-Verfahren kennt drei unterschiedliche Substitutionstabellen T_P, T_C und T_A, während die Original-Hill-Chiffre nur eine Substitutionstabelle $T_P = T_C$ kennt.

3.6 Unterschiede beim Angriff gegen Hill und gegen Hilly bei bekanntem K

Gegeben: Aus dem versendeten Geheimtext kann ein Angreifer einfach den eigentlichen Geheimtext C herausfiltern.
Er kann aber nicht einfach P = K^{-1} * C mod 26 berechnen, selbst wenn er K kennt, weil die Schlüsselmatrix K nicht invertierbar mod 26 ist.
Der Unterschied zum normalen Hillverfahren ist (abgesehen von der dynamischen Substitutionstabelle T_P und den Extensions):
Hill: C = K * P mod 26
Hilly: C1 = K * P (hier kein mod) und C = C1 mod 26
Es macht einen Unterschied, ob man mod 26 gleich anwendet oder erst auf das Ergebnis, weil im einen Fall die Schlüsselmatrix invertierbar mod 26 sein muss und im anderen Fall nicht.
Bei Hilly ist es also nicht möglich, die inverse Schlüsselmatrix mod 26 zu berechnen, da die Determinante der Schlüsselmatrix keine Inverse mod 26 besitzt.

Würde man bei Hilly die Prüfung $gcd(det(K), 26) \neq 1$ weglassen, würde das Verfahren weiterhin funktionieren. Man könnte es allerdings leicht angreifen, indem man die Buchstaben aus dem Geheimtext filtert und mit der invertierten Schlüsselmatrix mod 26 multipliziert [sofern für das zufällig gewählte K gelten würde $gcd(det(K), 26) = 1$].

3.7 Zur Invertierbarkeit einer Matrix

Wenn eine Matrix K invertierbar ist, dann ist auch E = x * I + K invertierbar, wobei x aus $\mathbb{N}$ ist und I die Einheitsmatrix der Seitenlänge n.

3.8 Zur Geheimtext-Länge

Hier ist der Geheimtext immer länger als der Klartext.

3.9 Zum Runden

Runden ist nur erforderlich, wenn es explizit angegeben ist (also in Schritt 9 der Verschlüsselung). Wenn beim Invertieren der Matrizen mit exakten Werten (Brüchen) gerechnet wird, ist Runden bei der Entschlüsselung nicht erforderlich.

Author of Hilly's Original Concept & Implementation: Yahya Almardeny