Hilly – An Improved Hill Cipher

Yahya Almardeny and Anna Lena Rotthaler

Version 1.0 – Jan 23, 2017

Contents

This challenge uses an improved version of the Hill cipher. The enhancement consists of a dynamic substitution table (step 2 and 3)(computed from the diagonal elements of the key matrix) and of an enhancement called the "extensions" (steps 9 to 14).
In contrast to the classical Hill cipher the key matrix should be just "invertible" but not invertible modulo 26. Therefore, the determinant of the key matrix may not equal 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25 mod 26 (so it must hold gcd(det(K), 26) $\neq$ 1). Positively said, the determinant may only have a value mod 26 from the following set: 2, 4, 6, 8, 10, 12, 13, 14, 16, 18, 20, 22, 24.

1 Encryption

1. Choose an invertible $n * n$-matrix K as key with $n \geq 5$ and $n = 6$ as default, at which K must hold: gcd(det(K), 26) $\neq$ 1.

2. Compute s as follows: Sum up the elements of the main diagonal of K (the main diagonal goes from top left to down right).
   If s=0: Sum up the elements of the secondary diagonal of K (the secondary diagonal goes from top right to down left).
   If also this s=0: Generate a new key matrix.

3. Compute the substitution table T_P for the plaintext-character alphabet:
   A=s, B=(2*s), C=(3*s), D=(4*s), ... , Z=(26*s)

4. Divide the plaintext into blocks of n characters.
   Please note that the plaintext length equals a multiple of n (see remark 3.4).

5. Replace the plaintext characters with numbers using the substitution table T_P. So you get the plaintext-number vector P.

6. Multiply K by P to get the vector C1: C1 = K * P

7. Compute the ciphertext vector C = C1 mod 26.

8. Substitute the elements in C using the substitution table T_C for the ciphertext alphabet: 0=Z, 1=A, 2=B, ..., 24=X, 25=Y.

9. Compute the "extension vector" X as follows: Divide C1 by 26 and round up the value: X = upperbound (C1 / 26)

10. The "extension matrix" E results by adding the value s to each element of K:
    E = s * I + K (I is the one matrix)

11. Compute the "encrypted extensions" X_{Enc} by multiplying E by X: $X_{Enc} = E * X$

12. Join all cipher letters with its encrypted extensions:
    C_1 X_{Enc1} ... C_6 X_{Enc6}

13. Define 11 additional symbols (one for each of the 10 decimal digits and one for the minus sign): (*, #, &, %, $, +, ?, !, @, ^, -). Then generate a substitution table T_A for these symbols as follows:

    a) Compute the sum t of all elements of the key matrix K mod 11.

    b) If the sum t equals zero, the substitution table T_A for additional symbols looks like this:

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

    Otherwise the symbols are shifted to the right by the result of step (a).

14. Substitute X_{Enc} using the substitution table T_A. So you get X_{EncSym}.

15. Send (C_1 $X_{EncSym1}$ ... C_6 $X_{EncSym6}$) to the recipient.

1.1 Example

Given: plaintext = 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. Substitution table T_P for plaintext-character 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. Concatenation: $\begin{pmatrix} J26270 \\ T25078 \\ P27740 \\ U27371 \\ H25247 \\ X28508 \end{pmatrix}$

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. Send the result of the last step as ciphertext.

2 Decryption

Given: the ciphertext in terms of (C_1 $X_{EncSym1}$ ... C_6 $X_{EncSym6}$) and the key matrix K.

1. Compute the diagonal sum s from K and compute the corresponding substitution table T_P for the plaintext-character alphabet.
2. Compute the sum of all elements of K mod 11 and the resulting substitution table T_A for additional symbols.
   Substitute the ciphertext characters using the substitution table T_A to get the "encrypted extensions" X_{Enc}.
3. Substitute all ciphertext letters from C using the substitution table T_C: A=1, B=2,..., Z=26.
4. The "extension matrix" E results by adding the value s to each element of K:
   E = s * I + K (I is the one matrix)
5. Compute the inverse K^{-1} of K and the inverse E^{-1} of E.
6. Multiply E^{-1} by X_{Enc} to get the "extension vector" X: $X = E^{-1} * X_{Enc}$
7. Use the following formula to compute C1, which was the result of the multiplication of the key matrix K by the substituted plaintext: C1 = (X * 26) - (26 - C)
8. Multiply K^{-1} by C1 (if you compute with the exact fractions, rounding is not necessary):
   $P = K^{-1} * C1$
9. Substitute P with the substitution table T_P.

2.1 Example

Given: ciphertext J@#@&?T@*?&%P@&&-?U@&^&!H@*@-&X@%*?% and key matrix 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 Remarks

3.1 About the substitution table T_P for the plaintext alphabet

Plaintext and ciphertext alphabet contain – like in the normal Hill cipher – the 26 capital letters each. s is defined in step 2.

- Because of s, the plaintext letters are not related to a fixed numerical value, but to a multiple of s.
- There are two different substitution tables – one for the plaintext alphabet T_P and one for the ciphertext alphabet T_C. The numerical values, which are related to the letters, are different:
  - T_P=(A=s, B=2*s, ..., Z=26*s) and
  - T_C=(0=Z, 1=A, 2=B, ..., 25=Y) [in case of encryption] and accordingly T_C=(1=A, 2=B, ... , Z=26) [in case of decryption].

3.2 About the substitution table T_C for the ciphertext alphabet

The substitution table T_C differs in encryption (step 8) and decryption (step 3). In encryption Z equals 0 and in decryption Z equals 26.
This is right, because in encryption X is computed as upperbound (C1 / 26). To undo the rounding in decryption, you have to subtract (26-C).
If C equals 0 in encryption, C1 is a multiple of 26 and to compute X there is no rounding needed. Therefore in decryption, for C=0 it has to be (26-C) = 0, because there has been no rounding and thus C must equal 26 in decryption.

3.3 About the substitution table T_A for additional symbols

The substitution table T_A consists of 11 symbols, one for each of the ten decimal digits and one for the minus sign.
In the ciphertext of the above example in this description there is no equivalent of the minus sign (which would be here the + character), because the values of the key matrix are all positive integers. If there are negative integers in the key matrix, there might be negative encrypted extensions and then there is the minus sign in the ciphertext. Therefore, it has to be in the substitution table T_A, because otherwise an attacker would get information about the key matrix.

3.4 Padding

3.4.1 Case encryption

If the plaintext length does not equal a multiple of n and you do not want the user to fill up the plaintext, padding is needed.

However, if the above named requirement (the plaintext length is a multiple of n) is fulfilled padding is not necessary.

Below, a manual method is described, which works up to a size of n=6. (For that purpose we establish yet another substitution table T_S: At a block length of n you need exactly n further symbols, which may occur neither in the plaintext alphabet nor in T_A. If you use very large matrices, you would run out of symbols.)

Repeat the last letter of the plaintext until the length is a multiple of n.
(Example: n = 6, EXAMPLE → EXAMPLEEEEEE)

To indicate, if padding has been used, do the following steps:

1. Calculate R = n - (number of letters of the plaintext mod n).
   (Example: R = 6 - (8 mod 6) = 6 - 2 = 4.)

2. If R = n, change it to R = 0 (no padding).

3. Substitute R using the following substitution table T_S for symbols:
   0 1 2 3 4 5
   ” \ : ; , .
   Add the symbol to the end of the ciphertext.
   (Example: The symbol in T_S for 4 is “ , ”. EXAMPLE → EXAMPLEEEEEE,)

3.4.2 Case decryption

Since the last character of the ciphertext is the symbol for R, this symbol and the corresponding R letters ahead of R of the decrypted text have to be removed to get the plaintext.

3.5 About the substitution tables in Hill and Hilly

The Hilly cipher knows three different substitution tables T_P, T_C, and T_A, while the original Hill cipher only knows one substitution table $T_P = T_C$.

3.6 Differences in attacks against Hill and Hilly with known K

Given: From the sent ciphertext an attacker can easily filter the actual ciphertext C.
But he cannot compute P = K^{-1} * C mod 26, even if he knows K, because the key matrix K is not invertible mod 26.
The difference to normal Hill cipher is (apart from the dynamic substitution table T_P and the extensions):
Hill: C = K * P mod 26
Hilly: C1 = K * P (no mod) and C = C1 mod 26
There is a difference, if you apply mod 26 directly or if you apply it to the result, because in the one case the key matrix has to be invertible mod 26 and in the other case not.
Therefore, at Hilly it is not possible to compute the inverse of the key matrix mod 26, because the determinant of the key matrix has no inverse mod 26.

If you omit the test $gcd(det(K), 26) \neq 1$, the procedure would still work. But you could easily attack it, when you filter the letters from the ciphertext and multiply them by the inverse of the key matrix mod 26 [if for the randomly chosen K the condition $gcd(det(K), 26) = 1$ would hold].

3.7 About the invertibility of a matrix

If a matrix K is invertible, E = x * I + K is also invertible, while x is from $\mathbb{N}$ and I is the one matrix with lateral length n.

3.8 About the ciphertext length

Here, the ciphertext is always longer than the plaintext.

3.9 About rounding

Rounding is only necessary, if explicitly mentioned (in step 9 of the encryption).
However, if the inverse of the matrices is computed with the exact values (fractions), rounding is not necessary in decryption.

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