

matrix and each of the five selected matrices in the module "Matrix" is implemented. The selected 8-letter words in the field of cryptography are COMPUTER, DOCUMENT, HARDWARE, SOFTWARE, SECURITY, ANALYSIS, DISCRETE, APPROACH (Figure 3). In the modulo "Decryption" the 8-letter encrypted English words are decrypted using the example matrix and each of the five selected valid matrices in the module "Matrix" is realized (Figure 4). The results of the operation of both modules are summarized in table 4.

Option	K	K ⁻¹
1	$\begin{pmatrix} 1 & 1 & 8 & 7 \\ 2 & 2 & 1 & 0 \\ 25 & 0 & 25 & 22 \\ 24 & 2 & 5 & 13 \end{pmatrix}$ det K=11	$\begin{pmatrix} 10 & 11 & 11 & 10 \\ 11 & 2 & 3 & 19 \\ 10 & 1 & 24 & 20 \\ 8 & 23 & 4 & 25 \end{pmatrix}$
2	$\begin{pmatrix} 4 & 1 & 8 & 7 \\ 2 & 2 & 1 & 0 \\ 25 & 0 & 25 & 22 \\ 24 & 2 & 5 & 13 \end{pmatrix}$ det K=3	$\begin{pmatrix} 2 & 23 & 23 & 2 \\ 23 & 23 & 24 & 5 \\ 2 & 13 & 10 & 12 \\ 12 & 17 & 24 & 3 \end{pmatrix}$
3	$\begin{pmatrix} 4 & 5 & 8 & 7 \\ 2 & 2 & 1 & 0 \\ 25 & 0 & 25 & 22 \\ 24 & 2 & 5 & 13 \end{pmatrix}$ det K=19	$\begin{pmatrix} 14 & 9 & 5 & 8 \\ 5 & 5 & 12 & 9 \\ 14 & 25 & 18 & 18 \\ 6 & 11 & 20 & 13 \end{pmatrix}$
4	$\begin{pmatrix} 4 & 5 & 8 & 7 \\ 2 & 2 & 1 & 0 \\ 25 & 4 & 25 & 22 \\ 24 & 2 & 5 & 13 \end{pmatrix}$ det K=21	$\begin{pmatrix} 4 & 25 & 7 & 16 \\ 7 & 23 & 23 & 2 \\ 15 & 23 & 24 & 5 \\ 8 & 23 & 4 & 25 \end{pmatrix}$
5	$\begin{pmatrix} 1 & 1 & 0 & 7 \\ 2 & 2 & 1 & 0 \\ 25 & 0 & 25 & 22 \\ 24 & 2 & 5 & 13 \end{pmatrix}$ det K=15	$\begin{pmatrix} 9 & 8 & 15 & 2 \\ 5 & 18 & 23 & 1 \\ 6 & 2 & 2 & 6 \\ 8 & 11 & 20 & 13 \end{pmatrix}$

Table 3: Selection of Matrix K and its inverse matrix K⁻¹.

No	Plaintext (Decrypted text)	Ciphertext (Option 1)	Ciphertext (Option 2)	Ciphertext (Option 3)	Ciphertext (Option 4)	Ciphertext (Option 5)
1	COMPUTER	OIPEUOAH	UIPEWOAH	UQPFCAH	UMPFCGAH	OIZFOUYG
2	DOCUMENT	PTGNVGAT	KTGNFGAT	YFGNFCAT	YNGNFCAT	PTINVGIT
3	HARDWARE	KNCUXEXI	FNCULEXI	FPCULOXI	FFCULEXI	KNYUXEDI
4	SOFTWARE	DGOPXEXI	FGOPLEXI	FAOPLOXI	FUOPLEXI	DGAPXEDI
5	SECURITY	KOMOSDLR	MOMORDLR	MIMORTLR	MQMORRLR	KOYOSDFR
6	ANALYSIS	EWQNSGG	EWQNKSGG	EWQNKGG	EWQNKQGG	EWQNSWGG
7	DISCRETE	JXYBYHLR	SXYBXHLR	SJYBXCLR	SDYBXVLR	JXBYHFR
8	APPROACH	HMHFYCPZ	HMHFOCPZ	HMHFOGPZ	HUHFOOPZ	HMHFYCHZ

Table 4: Results when encryption and Decryption of English texts using the application developed.

3Conclusion

This paper describes the classical Hill cipher to encrypt the English texts using 4x4 matrix. The application is developed based on MS EXCEL and the implementing processes of encryption and decryption of English texts using the Hill cipher is presented in details.

REFERENCES

- [1]V. Gellert, H. Kestner, Z. Noyber. Mathematical Encyclopedic Dictionary. Translation from German: N. Bozhinov and D. Minev, Sofia, Publishing House "Science and Art", 1983.
- [2]https://en.wikipedia.org/wiki/Hill_cipher
- [3]<http://www.practicalcryptography.com/ciphers/hill-cipher>
- [4]<http://crypto.interactive-maths.com/hill-cipher.html>
- [5]<http://writing.ufl.edu/3254/ExamplesandReadings/InstructionManualExample.doc>
- [6]<http://www.nku.edu/~christensen/092mat483%20hill%20cipher.pdf>
- [7]M. Eisenberg. Hill Ciphers and Modular Linear Algebra, <http://apprendre-en-ligne.net/crypto/hill/Hillciph.pdf>
- [8]Menezes, A.J., P.C. Van Oorschot, S.A. Van Stone. 1996. Handbook of Applied Cryptography. CRC press
- [9]Stalling, W. Cryptography and Network Security. 2005. 4th edition, Prentice Hall.
- [10]Adriana Naydenova Borodzhieva, MS Excel-Based Application for Encryption and Decryption of English Texts with the Hill Cipher on the Basis of 3x3-Matrix.



Md. Kamal Hossain Completed B.Sc in Telecommunication and Electronic Engineering from Hajee Mohammad Danesh Science and Technology University, Bangladesh. He is serving as a lecturer in the department of Electronics and Communication Engineering (Former Telecommunication and Electronic Engineering) at Hajee Mohammad Danesh Science and Technology University, Bangladesh. His research interest is Wireless Communication, Network Security.



Md. Ferdous Wahid Completed B.Sc in Electronics and Communication Engineering from Khulna University of Engineering & Technology. He is serving as a lecturer in the department of Electrical and Electronic Engineering at Hajee Mohammad Danesh Science and Technology University, Bangladesh. His research interest is Optical Fiber communication, Artificial Neural Network.