

ANIMOWANIE

MATEMATYKA

Autorki : Julia Taborska , Urszula Wolska

klasa 5a, Szkoła Podstawowa Nr 1 z Oddziałami Integrycyjnymi w Chrzanowie

ul. Borelowskiego 1, 32 – 500 Chrzanów

tel/fax 32623 28 44

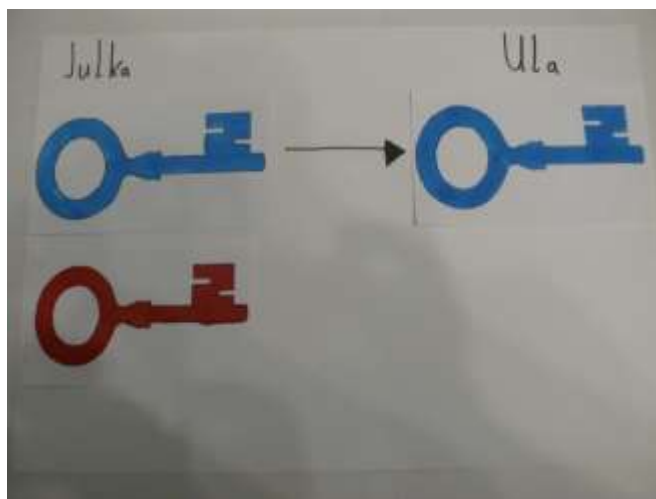
opiekun: Anna Szwancyber

Kryptograficzny algorytm szyfrujący pospolicie nazywamy szyfrem . Jest to funkcja matematyczna, która służy do szyfrowania lub deszyfrowania tekstu jawnego . Tekst jawny to zrozumiała informacja przed zaszyfrowaniem. Algorytm może być :

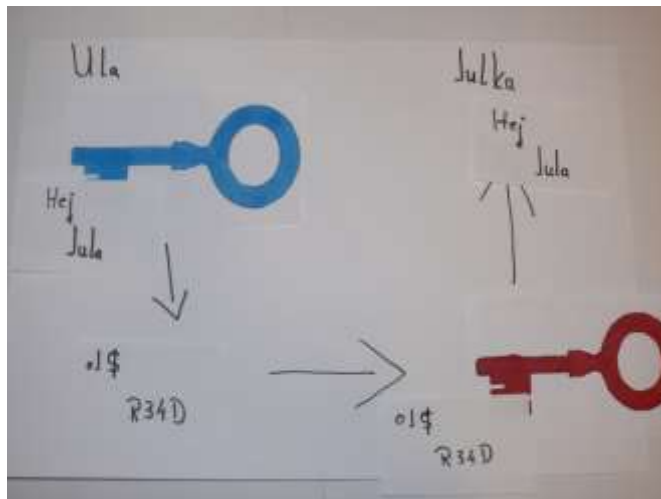
1. ograniczony - bezpieczeństwo szyfrogramu jest zapewnione wtedy kiedy nie jest znana postać algorytmu
2. algorytm z kluczem – bezpieczeństwo wiadomości oparte jest na kluczu (określa on przede wszystkim porządek liter w alfabecie szyfrowym, ustawienia na maszynie szyfrującej, wzorzec dokonywania zmian w przestawieniu)
 - a) algorytmy symetryczne – klucz szyfrujący może być określony z klucza deszyfrującego a klucz deszyfrujący wyznaczony z klucza szyfrującego

Możemy wyróżnić algorytmy strumieniowe oraz blokowe . W tych pierwszych informacja przetwarzana jest po jednym bicie , natomiast w drugich wiadomość przetwarzana jest blokami bitów (bit to najmniejsza ilość informacji potrzebna do określenia , który z dwóch równie prawdopodobnych stanów przyjął układ) . Przykłady szyfrów blokowych : DES, AES , BLOWFISH, DESX , IDEA, LUCIFER , MARS , SERPENT .

- b) algorytmy z kluczem publicznym – nie można określić klucza deszyfrującego z klucza szyfrującego , klucz publiczny (szyfrujący) nie jest taki sam jak klucz prywatny (deszyfrujący)



Julka przesyła swój klucz publiczny do Uli (klucz niebieski – klucz publiczny , klucz czerwony – klucz prywatny) .



Ula zaszyfruje wiadomość do Julki kluczem publicznym. Julka po otrzymaniu zaszyfrowanej informacji rozszyfruje ją swoim kluczem prywatnym.

Historia szyfrowania jest bardzo długa. Początkowo trzeba było stworzyć taki szyfr, który mógł być zaszyfrowany i deszyfrowany przez człowieka. Aktualnie większość tajnych wiadomości jest rozszyfrowywana przy pomocy komputerów. Przykładami szyfrów, które można używać do dzisiaj, bez zastosowania informatyki, z zapewnieniem jakiegokolwiek bezpieczeństwa są np.:

1. Szyfr z kluczem jednorazowym. Przykładem jest reguła Vernama. Wywodziła się z kodu Baudota, gdzie każdej literze odpowiadało pięć jednostek (impulsów). Zasugerował on wydziurkowanie na taśmie znaków klucza szyfrującego i elektromechaniczne dodawanie odpowiadających mu impulsów do tych, które odpowiadają znakom tekstu jawnego. Szyfrogram powstawał w wyniku procesu sumowania znaków:

<i>tekst jawny</i>	<i>klucz</i>	<i>szyfrogram</i>
plamka	+ plamka	= odstęp
plamka	+ odstęp	= plamka
odstęp	+ plamka	= plamka
odstęp	+ odstęp	= odstęp

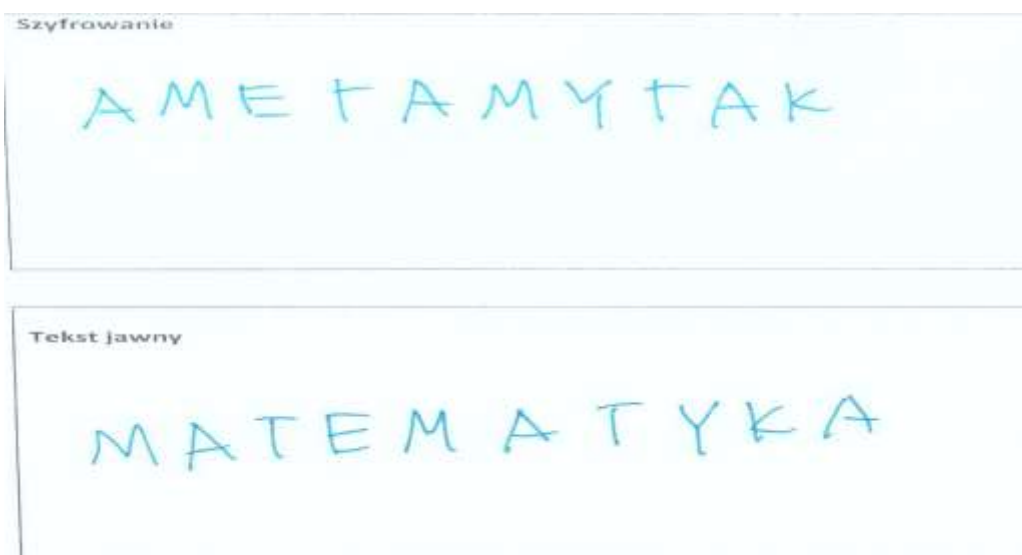
Celem prostszego posługiwania się szyfrem plamce przypisano cyfrę 1 , a odstępowi 0 .

		tekst jawny		
		1		0
klucz	1			szyfrogram
	0			

Vernam , aby uzyskać pięć impulsów dla znaków szyfrogramu połączył pięć impulsów odpowiadających znakom tekstu jawnego z pięcioma znakami klucza. Np.

tekst jawny	1	1	0	0	0
klucz	1	0	0	1	1
szyfrogram	0	1	0	1	1

2. Szyfry podstawieniowe . W wiadomości zaszyfrowanej znajdują się wszystkie znaki tekstu jawnego , ale w zmienionej kolejności np. (troszkę własnej twórczości) :



Szyfrowanie

EGGO BEAR

Tekst jawny

GEOGEBRA

Szyfry , które miały znaczenie w przeszłości :

a. Enigma



Maszyna wynaleziona na początku XX wieku przez doktora Arthura Scherbiusa. Urządzenie działało dzięki wirnikom. Miało tak wiele kluczy, że w razie potrzeby nie udałooby się przetestować na czas wszystkich możliwości . Dużą zasługą w rozszyfrowaniu urządzenia mieli Polscy uczeni : Marian Rejewski, Henryk Zygalski , Jerzy Różycki . Stworzyli metodę

określenia położenia wirników zestawiając pary liter i ustalili pozycje startową wirników .
 Rekonstruowali klucze dzienne dzięki czemu mogli rozszyfrowywać informację z danego dnia.

- b. Szyfr podstawieniowy (polegał na zastępowaniu każdego znaku tekstu jawnego innym znakiem szyfrogramu) . Wyróżniamy :
- prosty szyfr podstawieniowy (każdy znak tekstu jawnego zastępowany jest przez jeden znak szyfrogramu)
- Przykładem jest szyfr Cezara . Litery tekstu jawnego były zastępowane literami znajdującymi się o 3 miejsca dalej w alfabecie :

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

- homofoniczny szyfr podstawieniowy (poszczególny znak tekstu jawnego zastępowany jest odpowiadającym mu znakiem szyfrogramu) , np. szyfr Beale'a

71. 194. 38. 1701. 89. 76. 11. 83. 1628. 48. 94. 63. 132. 16. 111. 95. 84. 341. 975.
 14. 40. 64. 27. 81. 139. 213. 63. 90. 1120. 8. 15. 3. 126. 2018. 40. 74. 758. 485.
 604. 230. 436. 664. 582. 150. 251. 284. 308. 231. 124. 211. 486. 225. 401. 370.
 11. 101. 305. 139. 189. 17. 33. 80. 208. 193. 145. 1. 94. 73. 416. 918. 263. 28. 500.
 538. 256. 117. 136. 219. 27. 176. 130. 10. 460. 25. 485. 18. 436. 65. 84. 200. 293.
 118. 320. 138. 36. 416. 280. 15. 71. 224. 961. 44. 16. 401. 39. 801. 61. 204. 12. 23.
 24. 283. 134. 92. 63. 246. 486. 682. 7. 219. 184. 360. 780. 18. 64. 463. 474. 131.
 160. 79. 73. 440. 95. 18. 64. 581. 34. 69. 128. 367. 460. 17. 81. 12. 103. 820. 62.
 116. 97. 103. 862. 70. 60. 1317. 471. 540. 208. 121. 890. 346. 36. 150. 59. 568.
 614. 13. 120. 63. 219. 812. 2160. 1780. 99. 35. 18. 21. 136. 872. 15. 28. 170. 88. 4.
 30. 44. 112. 18. 147. 436. 195. 320. 37. 122. 113. 6. 140. 8. 120. 305. 42. 38. 461.
 64. 106. 301. 13. 408. 680. 93. 86. 116. 530. 82. 568. 9. 102. 38. 416. 89. 71. 216.
 728. 985. 818. 2. 38. 121. 195. 14. 328. 148. 234. 18. 35. 131. 234. 361. 824. 5.
 81. 623. 48. 961. 19. 26. 33. 10. 1101. 385. 92. 88. 181. 275. 346. 201. 206. 86.
 36. 219. 324. 829. 840. 64. 326. 19. 48. 122. 85. 218. 284. 919. 861. 326. 985.
 233. 64. 68. 232. 431. 980. 50. 29. 81. 214. 321. 603. 14. 612. 81. 360. 36. 51. 62.
 194. 78. 60. 200. 314. 676. 112. 4. 28. 18. 61. 136. 247. 819. 921. 1080. 464. 895.
 10. 6. 66. 119. 38. 41. 49. 602. 423. 962. 302. 294. 873. 78. 14. 23. 111. 109. 62.
 31. 501. 823. 216. 280. 34. 24. 150. 1000. 162. 286. 19. 21. 17. 340. 19. 242. 31.
 86. 234. 140. 607. 115. 33. 191. 67. 104. 86. 52. 88. 16. 80. 121. 67. 95. 122. 216.
 546. 96. 11. 201. 77. 364. 218. 65. 697. 890. 236. 154. 211. 10. 98. 34. 119. 56.
 216. 119. 71. 218. 1364. 1486. 1817. 51. 39. 210. 39. 1. 19. 540. 232. 22. 141. 617.
 84. 290. 80. 46. 207. 411. 150. 29. 38. 46. 172. 65. 194. 39. 261. 543. 897. 624. 18.
 212. 416. 127. 931. 19. 4. 63. 96. 12. 101. 418. 16. 140. 230. 460. 538. 15. 27. 88.
 612. 1431. 90. 716. 275. 74. 83. 11. 428. 89. 72. 84. 1300. 1706. 814. 221. 132.
 40. 102. 34. 888. 975. 1101. 84. 16. 79. 23. 16. 81. 122. 324. 403. 912. 227. 936.
 447. 55. 86. 34. 43. 212. 107. 96. 314. 264. 1065. 323. 428. 601. 203. 124. 95. 216.
 814. 2908. 654. 820. 2. 301. 112. 176. 213. 71. 87. 96. 202. 35. 10. 2. 41. 17. 84.
 221. 736. 820. 214. 11. 60. 760.

115. 73. 24. 807. 37. 52. 49. 17. 31. 62. 647. 22. 7. 15. 140. 47. 29. 107. 79. 84. 56.
 239. 15. 26. 811. 5. 196. 308. 85. 52. 180. 136. 58. 211. 36. 9. 46. 316. 554. 122.
 106. 95. 53. 58. 2. 42. 7. 35. 122. 53. 31. 81. 71. 250. 108. 36. 96. 118. 71. 148.
 287. 28. 323. 37. 1003. 65. 147. 807. 24. 1. 8. 12. 47. 43. 59. 887. 45. 316. 101. 41.
 78. 154. 1005. 122. 138. 131. 16. 77. 48. 182. 57. 72. 38. 73. 85. 35. 371. 59. 198.
 81. 92. 121. 106. 273. 90. 968. 620. 273. 225. 106. 388. 297. 83. 1. 191. 122. 43.
 234. 450. 106. 290. 314. 27. 48. 81. 98. 28. 115. 92. 156. 191. 210. 17. 85. 197. 46.
 15. 111. 140. 254. 48. 138. 108. 2. 607. 61. 438. 811. 29. 14. 24. 18. 17. 105. 38.
 248. 18. 159. 7. 35. 19. 83. 125. 110. 498. 287. 98. 117. 511. 62. 51. 120. 87. 113.
 125. 837. 18. 520. 84. 181. 67. 56. 6. 535. 127. 154. 248. 115. 61. 531. 15. 30. 5. 38. 8.
 603. 220. 7. 66. 154. 41. 7. 56. 6. 535. 127. 154. 248. 115. 61. 531. 15. 30. 5. 38. 8.
 14. 84. 57. 540. 217. 115. 71. 29. 84. 61. 43. 131. 29. 138. 47. 73. 239. 540. 52. 53.
 79. 118. 51. 44. 63. 198. 117. 259. 112. 1. 49. 79. 353. 100. 96. 373. 357. 211. 315.
 125. 380. 133. 143. 101. 15. 284. 540. 252. 34. 205. 140. 344. 36. 811. 138. 115.
 48. 73. 34. 205. 318. 607. 63. 220. 7. 52. 150. 44. 52. 16. 48. 37. 156. 807. 37. 121.
 12. 89. 10. 15. 85. 12. 133. 63. 115. 102. 897. 49. 53. 129. 138. 86. 31. 62. 67. 41.
 83. 83. 10. 100. 897. 138. 8. 115. 20. 32. 11. 11. 353. 207. 447. 47. 65. 50. 57. 49.
 47. 84. 6. 7. 71. 33. 4. 43. 47. 43. 1. 27. 695. 198. 230. 15. 191. 244. 85. 94. 511. 2.
 275. 25. 39. 7. 53. 44. 22. 40. 7. 10. 5. 811. 158. 44. 408. 239. 151. 111. 200. 11.
 15. 38. 42. 297. 61. 853. 136. 202. 698. 287. 6. 44. 53. 57. 511. 144. 10. 6. 256.
 577. 148. 13. 37. 54. 83. 47. 100. 86. 91. 847. 7. 44. 30. 11. 252. 10. 15. 35. 184.
 182. 113. 31. 102. 408. 239. 540. 320. 29. 64. 33. 101. 807. 138. 301. 316. 353.
 328. 220. 37. 52. 28. 540. 320. 33. 8. 48. 187. 50. 811. 7. 2. 113. 73. 16. 125. 11.
 118. 43. 102. 807. 31. 58. 81. 150. 58. 43. 445. 138. 19. 875. 688. 36. 45. 71. 14. 27.
 8. 47. 136. 63. 140. 44. 35. 22. 177. 108. 250. 314. 217. 2. 107. 7. 1068. 4. 20. 25.
 44. 48. 7. 26. 96. 130. 138. 807. 191. 34. 112. 347. 64. 110. 121. 275. 98. 41. 51.
 99. 148. 56. 47. 152. 348. 63. 807. 28. 42. 258. 138. 383. 98. 443. 52. 107. 140.
 112. 26. 85. 138. 540. 51. 20. 125. 371. 39. 36. 10. 52. 114. 136. 161. 420. 151.
 112. 71. 14. 33. 7. 34. 18. 12. 807. 37. 67. 138. 62. 53. 21. 83. 271. 152. 811.
 83. 81. 84. 105. 655. 13. 2. 108. 230. 196. 151. 105. 106. 65. 175. 71. 8. 52. 238.
 145. 117. 125. 540. 65. 13. 2. 108. 230. 196. 151. 105. 106. 65. 175. 71. 8. 52. 238.
 154. 315. 46. 106. 314. 275. 305. 101. 811. 488. 8. 44. 37. 52. 46. 241. 34. 203.
 38. 16. 46. 47. 65. 24. 44. 15. 64. 73. 138. 807. 85. 78. 110. 31. 420. 565. 33. 17.
 38. 22. 31. 10. 110. 108. 180. 140. 15. 38. 1. 5. 64. 7. 68. 287. 125. 150. 98. 33. 84.
 123. 807. 191. 96. 511. 118. 440. 370. 643. 466. 106. 41. 187. 463. 220. 275. 38.
 150. 105. 49. 53. 287. 258. 268. 134. 7. 53. 12. 47. 85. 63. 136. 110. 21. 112. 140.
 483. 486. 105. 14. 73. 84. 375. 1005. 150. 206. 16. 62. 5. 4. 25. 42. 8. 18. 811.
 123. 180. 12. 203. 803. 887. 61. 98. 893. 41. 880. 136. 14. 20. 28. 28. 533. 802.
 248. 8. 131. 180. 140. 344. 440. 42. 18. 811. 48. 67. 101. 102. 194. 138. 203. 51.
 83. 241. 540. 122. 4. 15. 83. 140. 47. 48. 148. 288.

- poligramowy szyfr podstawieniowy (szyfrowane są grupy znaków zamiast pojedynczych)

Szyfr Giovanni Battisty Porty , w którym zastąpił każdą parę liter znakiem w miejscu przecięcia się wierszy i kolumn.

| | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A | B | C | D | E | F | G | H | I | L | M | N | O | P | Q | R | S | T | V | Z | |
| Y | Q | Y | 9 | V | H | W | 0 | X | 0 | X | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | A |
| 0 | P | Δ | P | Δ | H | 0 | X | 0 | 0 | X | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | B |
| 0 | 0 | X | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | C |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | D |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | E |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | F |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | G |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | H |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | I |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | L |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | M |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | N |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | O |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | P |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | Q |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | R |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | S |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | T |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | V |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | Z |

- polialfabetyczny szyfr podstawieniowy (powstaje w wyniku złożenia kilku szyfrów monoalfabetycznych)

Szyfr Vigenera . Podobny jest do szyfru Cezara. Przesunięcie kolejno wynosi 0, 1, 2 itd. Do zaszyfrowania wiadomości potrzebne jest słowo kluczowe, które jest tajne.

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

c. Szachownica Polibiusza

Grecki pisarz Polibiusz poukładał litery w kwadrat. Ponumerował wiersze i kolumny . Jedna litera była odpowiednikiem dwóch cyfr . Modyfikacja dla polskiego alfabetu .

| | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| 1 | a | b | c | d | e |
| 2 | f | g | h | i | j |
| 3 | k | l | ł | m | n |
| 4 | o | p | r | s | t |
| 5 | u | w | x | y | z |

Nasze zaszyfrowane wiadomości :

Szyfrowanie

22 15 41 22 15 12 43 11

Tekst jawny

GEOGEBRA

Szyfrowanie

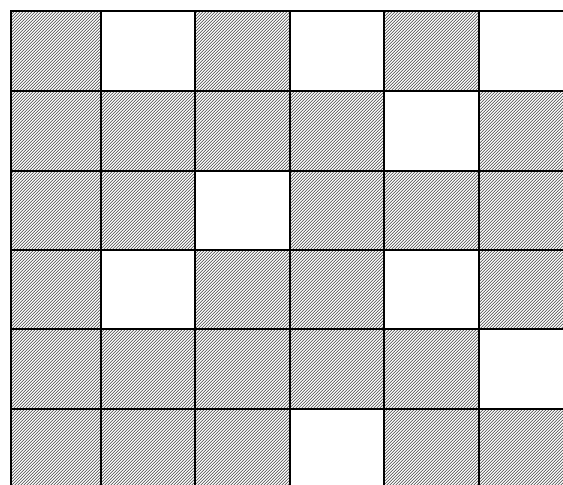
34 11 45 15 34 11 45 54 31 11

Tekst jawny

M A T E M A T Y K A

e) maskownica obrotowa Cardana

Był to zazwyczaj kawałek kartonu. Został on podzielony na małe pola – kwadraty, z których $\frac{1}{4}$ została wycięta tworząc szablon. W puste pola wpisywano hasło. Następnie obracano 3 razy o 90 stopni, za każdym razem wpisując litery. Wiadomość zazwyczaj odczytywano wierszami.



Wspólnie wymyśliłyśmy zaszyfrowaną wiadomość :

| | | | | | |
|---|---|---|---|---|---|
| A | M | R | A | T | T |
| Z | O | Z | S | E | K |
| V | E | M | O | D | P |
| L | A | E | M | T | N |
| R | I | Y | P | ! | Y |
| O | ! | T | K | S | ! |



W czasie szyfrowania ...



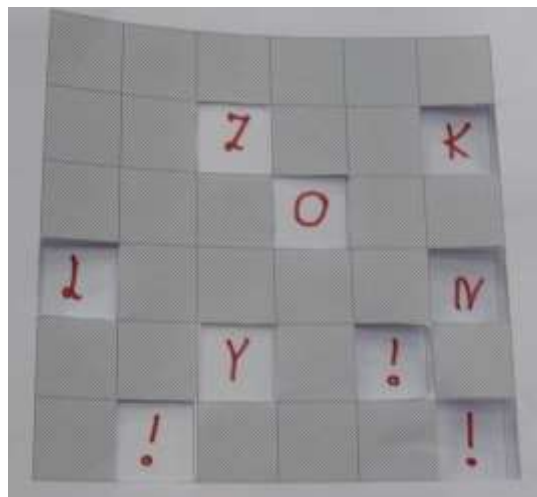
MATEMATYK



A TO SUPER P



RZEDMIOT S



ZKOLNY !!!

Rozszyfrowana wiadomość : MATEMATYKA TO SUPER PRZEDMIOT SZKOLNY !!!

Podsumowanie:

W tej prezentacji przedstawiliśmy dużo szyfrów z wielu epok. Chciałyśmy pokazać, iż szyfrowanie było tak naprawdę od zawsze i towarzyszy nam do dzisiaj w różnych celach. Kilka kodów wypróbowałyśmy same, co miało udowodnić, iż czasami poufne wiadomości można przedstawić w prosty sposób, a do ich rozwiązania nie trzeba używać komputera. Pragniemy również zaznaczyć, że szyfrowanie jest bardzo atrakcyjną, logiczną rozrywką dla naszych młodych umysłów.

Bibliografia:

- „Łamacze szyfrów” – David Kahn
- Wikipedia (przede wszystkim) :
 - <https://pl.wikipedia.org/wiki/Szyfr>
 - https://pl.wikipedia.org/wiki/Algorytm_symetryczny
 - https://pl.wikipedia.org/wiki/Szyfr_strumieniowy
 - https://pl.wikipedia.org/wiki/Szyfr_blokowy
 - https://pl.wikipedia.org/wiki/Kryptografia_klucza_publicznego
 - <https://pl.wikipedia.org/wiki/Enigma>
 - https://pl.wikipedia.org/wiki/Szyfr_podstawieniowy
 - https://pl.wikipedia.org/wiki/Szyfr_monoalfabetyczny
 - https://pl.wikipedia.org/wiki/Szyfr_homofoniczny
 - https://pl.wikipedia.org/wiki/Szyfr_poligramowy
 - https://pl.wikipedia.org/wiki/Szyfr_polialfabetyczny
 - https://pl.wikipedia.org/wiki/Szyfr_przestawieniowy
 - https://pl.wikipedia.org/wiki/Szachownica_Polibiusza