#### Система шифрования Вижинера

Система Вижинера впервые была опубликована в 1586 г. и является одной из старейших и наиболее известных многоалфавитных систем. Свое название она получила по имени французского дипломата XVI века Блеза Вижинера, который развивал и совершенствовал криптографические системы.

Система Вижинера подобна такой системе шифрования Цезаря, у которой ключ подстановки меняется от буквы к букве. Этот шифр многоалфавитной замены можно описать таблицей шифрования, называемой таблицей (квадратом) Вижинера. На рис. 2.8 и 2.9 показаны таблицы Вижинера для русского и английского алфавитов соответственно.

Таблица Вижинера используется для зашифрования и расшифрования. Таблица имеет два входа:

* верхнюю строку подчеркнутых символов, используемую для считывания очередной буквы исходного открытого текста;
* крайний левый столбец ключа.

Последовательность ключей обычно получают из числовых значений букв ключевого слова.

При шифровании исходного сообщения его выписывают в строку, а под ним записывают ключевое слово (или фразу). Если ключ оказался короче сообщения, то его циклически повторяют. В процессе шифрования находят в верхней строке таблицы очередную букву исходного текста и в левом столбце очередное значение ключа. Очередная буква шифртекста находится на пересечении столбца, определяемого шифруемой буквой, и строки, определяемой числовым значением ключа.

Пусть ключевая последовательность имеет длину r, тогда ключ r-алфавитной подстановки есть r-строка

 = (π0, π1, …, πr–1). (2.9)

Система шифрования Вижинера преобразует открытый текст  = (x0, x1, …, xn–1) в шифртекст  = (y0, y1, …, yn–1) с помощью ключа  = (π0, π1, …, πn–1) согласно правилу

Tπ :  = (x0, x1, …, xn–1) →  = (y0, y1, …, yn–1),

(y0, y1, …, yn–1) = (π0 (x0), π1 (x1), …, πn–1(xn–1)), (2.10)

где πi = π(i mod r).

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **а** | **б** | **в** | **г** | **д** | **е** | **ж** | **з** | **и** | **й** | **к** | **л** | **м** | **н** | **о** | **п** | **р** | **с** | **т** | **у** | **ф** | **х** | **ц** | **ч** | **ш** | **щ** | **ь** | **ы** | **ъ** | **э** | **ю** | **я** |
| **Ключ** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **0** | а | б | в | г | д | е | ж | з | и | й | к | л | м | н | о | п | р | с | т | у | ф | х | ц | ч | ш | щ | ь | ы | ъ | э | ю | я |
| **1** | б | в | г | д | е | ж | з | и | й | к | л | м | н | о | п | р | с | т | у | ф | х | ц | ч | ш | щ | ь | ы | ъ | э | ю | я | а |
| **2** | в | г | д | е | ж | з | и | й | к | л | м | н | о | п | р | с | т | у | ф | х | ц | ч | ш | щ | ь | ы | ъ | э | ю | я | а | б |
| **3** | г | д | е | ж | з | и | й | к | л | м | н | о | п | р | с | т | у | ф | х | ц | ч | ш | щ | ь | ы | ъ | э | ю | я | а | б | в |
| **4** | д | е | ж | з | и | й | к | л | м | н | о | п | р | с | т | у | ф | х | ц | ч | ш | щ | ь | ы | ъ | э | ю | я | а | б | в | г |
| **5** | е | ж | з | и | й | к | л | м | н | о | п | р | с | т | у | ф | х | ц | ч | ш | щ | ь | ы | ъ | э | ю | я | а | б | в | г | д |
| **6** | ж | з | и | й | к | л | м | н | о | п | р | с | т | у | ф | х | ц | ч | ш | щ | ь | ы | ъ | э | ю | я | а | б | в | г | д | е |
| **7** | з | и | й | к | л | м | н | о | п | р | с | т | у | ф | х | ц | ч | ш | щ | ь | ы | ъ | э | ю | я | а | б | в | г | д | е | ж |
| **8** | и | й | к | л | м | н | о | п | р | с | т | у | ф | х | ц | ч | ш | щ | ь | ы | ъ | э | ю | я | а | б | в | г | д | е | ж | з |
| **9** | й | к | л | м | н | о | п | р | с | т | у | ф | х | ц | ч | ш | щ | ь | ы | ъ | э | ю | я | а | б | в | г | д | е | ж | з | и |
| **10** | к | л | м | н | о | п | р | с | т | у | ф | х | ц | ч | ш | щ | ь | ы | ъ | э | ю | я | а | б | в | г | д | е | ж | з | и | й |
| **11** | л | м | н | о | п | р | с | т | у | ф | х | ц | ч | ш | щ | ь | ы | ъ | э | ю | я | а | б | в | г | д | е | ж | з | и | й | к |
| **12** | м | н | о | п | р | с | т | у | ф | х | ц | ч | ш | щ | ь | ы | ъ | э | ю | я | а | б | в | г | д | е | ж | з | и | й | к | л |
| **13** | н | о | п | р | с | т | у | ф | х | ц | ч | ш | щ | ь | ы | ъ | э | ю | я | а | б | в | г | д | е | ж | з | и | й | к | л | м |
| **14** | о | п | р | с | т | у | ф | х | ц | ч | ш | щ | ь | ы | ъ | э | ю | я | а | б | в | г | д | е | ж | з | и | й | к | л | м | н |
| **15** | п | р | с | т | у | ф | х | ц | ч | ш | щ | ь | ы | ъ | э | ю | я | а | б | в | г | д | е | ж | з | и | й | к | л | м | н | о |
| **16** | р | с | т | у | ф | х | ц | ч | ш | щ | ь | ы | ъ | э | ю | я | а | б | в | г | д | е | ж | з | и | й | к | л | м | н | о | п |
| **17** | с | т | у | ф | х | ц | ч | ш | щ | ь | ы | ъ | э | ю | я | а | б | в | г | д | е | ж | з | и | й | к | л | м | н | о | п | р |
| **18** | т | у | ф | х | ц | ч | ш | щ | ь | ы | ъ | э | ю | я | а | б | в | г | д | е | ж | з | и | й | к | л | м | н | о | п | р | с |
| **19** | у | ф | х | ц | ч | ш | щ | ь | ы | ъ | э | ю | я | а | б | в | г | д | е | ж | з | и | й | к | л | м | н | о | п | р | с | т |
| **20** | ф | х | ц | ч | ш | щ | ь | ы | ъ | э | ю | я | а | б | в | г | д | е | ж | з | и | й | к | л | м | н | о | п | р | с | т | у |
| **21** | х | ц | ч | ш | щ | ь | ы | ъ | э | ю | я | а | б | в | г | д | е | ж | з | и | й | к | л | м | н | о | п | р | с | т | у | ф |
| **22** | ц | ч | ш | щ | ь | ы | ъ | э | ю | я | а | б | в | г | д | е | ж | з | и | й | к | л | м | н | о | п | р | с | т | у | ф | х |
| **23** | ч | ш | щ | ь | ы | ъ | э | ю | я | а | б | в | г | д | е | ж | з | и | й | к | л | м | н | о | п | р | с | т | у | ф | х | ц |
| **24** | ш | щ | ь | ы | ъ | э | ю | я | а | б | в | г | д | е | ж | з | и | й | к | л | м | н | о | п | р | с | т | у | ф | х | ц | ч |
| **25** | щ | ь | ы | ъ | э | ю | я | а | б | в | г | д | е | ж | з | и | й | к | л | м | н | о | п | р | с | т | у | ф | х | ц | ч | ш |
| **26** | ь | ы | ъ | э | ю | я | а | б | в | г | д | е | ж | з | и | й | к | л | м | н | о | п | р | с | т | у | ф | х | ц | ч | ш | щ |
| **27** | ы | ъ | э | ю | я | а | б | в | г | д | е | ж | з | и | й | к | л | м | н | о | п | р | с | т | у | ф | х | ц | ч | ш | щ | ь |
| **28** | ъ | э | ю | я | а | б | в | г | д | е | ж | з | и | й | к | л | м | н | о | п | р | с | т | у | ф | х | ц | ч | ш | щ | ь | ы |
| **29** | э | ю | я | а | б | в | г | д | е | ж | з | и | й | к | л | м | н | о | п | р | с | т | у | ф | х | ц | ч | ш | щ | ь | ы | ъ |
| **30** | ю | я | а | б | в | г | д | е | ж | з | и | й | к | л | м | н | о | п | р | с | т | у | ф | х | ц | ч | ш | щ | ь | ы | ъ | э |
| **31** | я | а | б | в | г | д | е | ж | з | и | й | к | л | м | н | о | п | р | с | т | у | ф | х | ц | ч | ш | щ | ь | ы | ъ | э | ю |

Рис. 2.8. Таблица Вижинера для русского алфавита

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **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** |
| **Ключ** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **0** | 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 |
| **1** | 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 |
| **2** | 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 |
| **3** | 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 |
| **4** | 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 |
| **5** | 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 |
| **6** | 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 |
| **7** | 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 |
| **8** | 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 |
| **9** | 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 |
| **10** | 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 |
| **11** | 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 |
| **12** | 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 |
| **13** | 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 |
| **14** | 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 |
| **15** | 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 |
| **16** | 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 |
| **17** | 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 |
| **18** | 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 |
| **19** | 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 |
| **20** | 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 |
| **21** | 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 |
| **22** | 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 |
| **23** | 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 |
| **24** | 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 |
| **25** | 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 |

Рис. 2.9. Таблица Вижинера для английского алфавита

Рассмотрим пример получения шифртекста с помощью таблицы Вижинера. Пусть выбрано ключевое слово АМБРОЗИЯ. Необходимо зашифровать сообщение ПРИЛЕТАЮ СЕДЬМОГО.

Выпишем исходное сообщение в строку и запишем под ним ключевое слово с повторением. В третью строку будем выписывать буквы шифртекста, определяемые из таблицы Вижинера.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Сообщение | П | Р | И | Л | Е | Т | А | Ю | С | Е | Д | Ь | М | О | Г | О |
| Ключ | А | М | Б | Р | О | З | И | Я | А | М | Б | Р | О | З | И | Я |
| Шифртекст | П | Ъ | Й | Ы | У | Щ | И | Э | С | С | Е | К | Ь | Х | Л | Н |