Лабораторна робота 5

Тема. Дослідження алгоритму шифрування

**з відкритим ключем RSA**

Завдання.

1. Вивчити:

стандарт криптографічного перетворення з відкритим ключем RSA, правила обчислення відкритого і закритого криптографічних ключів, прямого і оберненого криптографічних перетворень.

1. Розробити структури даних і реалізувати алгоритм RSA.
2. Апробувати процес зашифрування і розшифрування різних варіантів тексту на різних криптографічних ключах за алгоритмом RSA:

а) ввести в режимі ручного введення текст для шифрування довжиною не більше 240 символів;

б) виконати процедуру обчислення і вивести на екран відкритий та закритий (секретний) криптографічні ключі для шифрування або ввести їх в режимі ручного введення;

в) представити введений відкритий текст як послідовність чисел у відповідності з обраним модулем криптографічного перетворення;

г) виконати процес зашифрування і розшифрування введеного відкритого тексту, отримати результати за всіма етапами шифрування на екрані дисплея;

д) впевнитися у коректності роботи програми, правильності виконання обчислень, порівняти первинний відкритий текст з результатом розшифрування його криптограми;

е) повторити пункти а−д для нових відкритих текстів та криптографічних ключів різної довжини;

ж) виконати пункти а−д для оригінальних відкритого тексту і криптографічних ключів.

Текст для шифрування та початкові значення простих чисел *p* і *q* для обчислення відкритого (*E*) і закритого (*D*) криптографічних ключів приведено в таблицях 3 і 4. Варіант тексту для шифрування визначається за передостанньою цифрою (*i*) номера залікової книжки (таблиця 3). Варіант значень *p* і *q* визначається за останньою (*j*) цифрою номера залікової книжки (таблиця 4). Отримані ключі *e* і *d* повинні задовольняти умові: *e* > 7 и *e* ≠ *d*.

 Таблиця 3 Таблиця 4

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| *i* | Текст для шифрування |  | *j* | Значення *p* | Значення *q* |
| 0 | ВЗЛОМ |  | 0 | 3 | 17 |
| 1 | ВИРУС |  | 1 | 3 | 19 |
| 2 | ДАТЧИК |  | 2 | 3 | 23 |
| 3 | ДОСТУП |  | 3 | 3 | 29 |
| 4 | МЕТОД |  | 4 | 5 | 11 |
| 5 | ОБЪЕКТ |  | 5 | 5 | 17 |
| 6 | ПАРОЛЬ |  | 6 | 7 | 17 |
| 7 | ПЭМИН |  | 7 | 7 | 19 |
| 8 | РЕЖИМ |  | 8 | 13 | 17 |
| 9 | СЕКРЕТ |  | 9 | 19 | 29 |

Числові зображення (еквіваленти) літер російського алфавиту представлені в таблиці 5.

Таблиця 5

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Буква | Число | Буква | Число | Буква | Число |
| А | 1 | К | 12 | Х | 23 |
| Б | 2 | Л | 13 | Ц | 24 |
| В | 3 | М | 14 | Ч | 25 |
| Г | 4 | Н | 15 | Ш | 26 |
| Д | 5 | О | 16 | Щ | 27 |
| Е | 6 | П | 17 | Ъ | 28 |
| Ё | 7 | Р | 18 | Ы | 29 |
| Ж | 8 | С | 19 | Ь | 30 |
| З | 9 | Т | 20 | Э | 31 |
| И | 10 | У | 21 | Ю | 32 |
| Й | 11 | Ф | 22 | Я | 33 |

Прості числа від 2 до 2239 представлені в таблиці 6.

Таблиця 6

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 2 | 163 | 379 | 613 | 859 | 1109 | 1409 | 1657 | 1951 |
| 3 | 167 | 383 | 617 | 863 | 1117 | 1423 | 1663 | 1973 |
| 5 | 173 | 389 | 619 | 877 | 1123 | 1427 | 1667 | 1979 |
| 7 | 179 | 397 | 631 | 881 | 1129 | 1429 | 1669 | 1987 |
| 11 | 181 | 401 | 641 | 883 | 1151 | 1433 | 1693 | 1993 |
| 13 | 191 | 409 | 643 | 887 | 1153 | 1439 | 1697 | 1997 |
| 17 | 193 | 419 | 647 | 907 | 1163 | 1447 | 1699 | 1999 |
| 19 | 197 | 421 | 653 | 911 | 1171 | 1451 | 1709 | 2003 |
| 23 | 199 | 431 | 659 | 919 | 1181 | 1453 | 1721 | 2011 |
| 29 | 211 | 433 | 661 | 929 | 1187 | 1459 | 1723 | 2017 |
| 31 | 223 | 439 | 673 | 937 | 1193 | 1471 | 1733 | 2027 |
| 37 | 227 | 443 | 677 | 941 | 1201 | 1481 | 1741 | 2029 |
| 41 | 229 | 449 | 683 | 947 | 1213 | 1483 | 1747 | 2039 |
| 43 | 239 | 457 | 691 | 953 | 1217 | 1487 | 1753 | 2053 |
| 47 | 233 | 461 | 701 | 967 | 1223 | 1489 | 1759 | 2063 |
| 53 | 241 | 463 | 709 | 971 | 1229 | 1493 | 1777 | 2069 |
| 59 | 251 | 467 | 719 | 977 | 1231 | 1499 | 1783 | 2081 |
| 61 | 257 | 479 | 727 | 983 | 1237 | 1511 | 1787 | 2083 |
| 67 | 263 | 487 | 733 | 991 | 1249 | 1523 | 1789 | 2087 |
| 71 | 269 | 491 | 739 | 997 | 1259 | 1531 | 1801 | 2089 |
| 73 | 271 | 499 | 743 | 1009 | 1277 | 1543 | 1811 | 2099 |
| 79 | 277 | 503 | 751 | 1013 | 1279 | 1549 | 1823 | 2111 |
| 83 | 281 | 509 | 757 | 1019 | 1283 | 1553 | 1831 | 2113 |
| 89 | 283 | 521 | 761 | 1021 | 1289 | 1559 | 1847 | 2129 |
| 97 | 293 | 523 | 769 | 1031 | 1291 | 1567 | 1861 | 2131 |
| 101 | 307 | 541 | 773 | 1033 | 1297 | 1571 | 1867 | 2137 |
| 103 | 311 | 547 | 787 | 1039 | 1301 | 1579 | 1871 | 2141 |
| 107 | 313 | 557 | 797 | 1049 | 1303 | 1583 | 1873 | 2143 |
| 109 | 317 | 563 | 809 | 1051 | 1307 | 1597 | 1877 | 2153 |
| 113 | 331 | 569 | 811 | 1061 | 1319 | 1601 | 1879 | 2161 |
| 127 | 337 | 571 | 821 | 1063 | 1321 | 1607 | 1889 | 2179 |
| 131 | 347 | 577 | 823 | 1069 | 1327 | 1609 | 1901 | 2203 |
| 137 | 349 | 587 | 827 | 1087 | 1361 | 1613 | 1907 | 2207 |
| 139 | 353 | 593 | 829 | 1091 | 1367 | 1619 | 1913 | 2213 |
| 149 | 359 | 599 | 839 | 1093 | 1373 | 1621 | 1931 | 2221 |
| 151 | 367 | 601 | 853 | 1097 | 1381 | 1627 | 1933 | 2237 |
| 157 | 373 | 607 | 857 | 1103 | 1399 | 1637 | 1949 | 2239 |