# CONTROL DE TRANSMISIÓN DE DATOS
11 de diciembre de 2003
GRUPO 10

NOTA IMPORTANTE:

- *Un **error conceptual grave** puede anular todo el problema.*

PROBLEMA 1

Sea un sistema de RSA en el que la clave pública del usuario B vale (N=7663, e=4831). Utilice la tabla adjunta cuando lo crea necesario:

a) Calcule $X = 397^{1982} \bmod 991$. Justifique cómo ha realizado el cálculo. **(1,5 puntos)**

b) Decodifique el criptograma C=000000000101, enviado por el usuario A al usuario B. **(2 puntos)**

c) Cifre el mensaje M=222 con la secuencia generada por un LFSR caracterizado por el polinomio primitivo $C(D) = D^7 + D + 1$. La clave de sesión determina el estado inicial del LFSR (en este caso $S(D) = D + 1$). Indique posibles debilidades de este cifrador en flujo síncrono, así como la longitud máxima de mensaje que podría cifrarse con una misma clave de sesión. **(1.5 puntos)**

PROBLEMA 2

Sea una fuente de información con memoria cuyo alfabeto es de 3 símbolos {A, B, C} con p(A|A)=0,5; p(B|A)=0,25; p(A|B)=p(B|B)=0,5; p(A|C)=0,25; p(B|C)=0.

a) Calcule la relación señal a ruido mínima a la entrada del receptor (en escala lineal) para que sea posible transmitir 10.000 símbolos de fuente por un canal de W=1KHz en un tiempo de 2 segundos. **(1,5 puntos)**

b) Decodifique la secuencia 1124670 mediante un codificador de LZW, con un diccionario cargado inicialmente con A en la posición 0, B en la 1 y C en la 2. Indique la secuencia de salida y el diccionario creado en recepción. **(1,5 puntos)**

c) Realice una codificación de Huffman (binaria) de la fuente extendida de orden 2. Calcule la eficiencia de codificación. **(2 puntos)**

**Table 8.1** Primes under 2000

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