**Какие разряды регистра будут участвовать в формировании вдвигаемого в первый разряд значения?** (ненулевые коэффициенты  многочлена определяют разряды регистра, которые будут участвовать в формировании вдвигаемого в первый разряд значения)

**Чему равен максимально возможный период?** (2*m* – 1, где m – количество разрядов регистра, степень многочлена). **Чему равно количество разрядов регистра?** (степень многочлена)

**Что называется М-последовательностью?** (Последовательность максимально возможного для данного генератора периода называется M-последовательностью)

**Выход генератора Геффе *xG* описывается так: *xG*= (*x*1 *and* x2) *or* (*not* *x*1 *and* *x*3).** Период данного генератора равен (2*m1* – 1)(2*m2* – 10)(2*m3* – 1), где *m*1, *m*2 и *m*3 – длины первого, второго и третьего LFSR соответственно.

**Начальная длина ключа?**

**Вариант 1**

|  |
| --- |
|  |
| 11111111 11111111 11111110 00001111 10000011 11100011 …. – выходной ключ (до-1) |

**Вариант 2**

|  |
| --- |
|  |
| 11111111 11111111 11111111 01000010 11110100 00 …. – выходной ключ (до-1) |

**Вариант 3**

|  |
| --- |
|  |
| 11111111 11111111 11111111 10001110 00111000 11100011 …- выходной ключ (до-1) |

**Вариант 4**

|  |
| --- |
| **LFSR1 =** |
| 11111111 11111111 11111111 11010101 00000000 10101011 …– выходной ключ (до-1) |

**Вариант 5**

|  |
| --- |
| **LFSR1 =** |
| 11111111 11111111 11111111 11101010 10000000 01010101 …– выходной ключ (до-1) |

**Вариант 6**

|  |
| --- |
| **LFSR1 =** |
| 11111111 11111111 11111111 11110001 11000111 00011100 …– выходной ключ (до-1) |

**Вариант 7**

|  |
| --- |
|  |
| 11111111 11111111 11111111 11111001 10011001 10011001 …- выходной ключ (до-1) |

**Вариант 8**

|  |
| --- |
| **LFSR1 =** |
| 11111111 11111111 11111111 11111101 01010101 01010000 …– выходной ключ (до-1) |

**Вариант 9**

|  |
| --- |
| **LFSR1 = а** |
| 11111111 11111111 11111111 11111110 00111000 11100011 10001110 00111011 … |

**Вариант 10**

|  |
| --- |
| **LFSR1 = ы** |
| 11111111 11111111 11111111 11111111 01010101 0101 …– выходной ключ (до-1) |

**Вариант 11**

|  |
| --- |
| **LFSR1 = ы** |
| 11111111 11111111 11111111 11111111 10000000 00000011 11111111 111 … |

**Вариант 12**

|  |
| --- |
| **LFSR1 = ы** |
| 11111111 11111111 11111111 11111111 11010101 01010101 111111111 … |

**Вариант 13**

|  |
| --- |
| **LFSR1 =** |
| 11111111 11111111 11111111 11111111 11100110 01100110 01100110 … |

**Вариант 14**

|  |
| --- |
| **LFSR1 =** |
| 11111111 11111111 11111111 11111111 11110000 00000001 11111111 11... |

**Вариант 15**

|  |
| --- |
| **LFSR1 =** |
| 11111111 11111111 11111111 11111111 11111001 10011000 00000000 011 … |

**Вариант 16**

|  |
| --- |
| **LFSR1 =** |
| 11111111 11111111 11111111 11111111 111111 01010000 00101011 1111.. |

**Вариант 17**

|  |
| --- |
| **LFSR1 =** |
| 11111111 11111111 11111111 11111111 11111110 00011110 00011110 00011110 … |

**Вариант 18**

|  |
| --- |
| **LFSR1 =** |
| 11111111 11111111 11111111 11111111 11111111 0011001100 1100110011 .. |

**RС4: RC4:**

**U= 0 1 2 3 4 U= 1 2 3 4 5**

**K= 254 29 11 51 228 K= 178 57 99 5 240**