1. Используя нек. вектор S = (103, 107, 211, 430, 863, 1716, 3449, 6907, 13807, 27610), вычислить ключи для зашифрования и расшифрования сообщений (ранцевый алг)

ΣS = 55203  
Выберем простое число (q=58147), превосходящее ΣS и (r=1007) из интервала [1; ΣS]  
НОД(q,r) = 1, числа взаимно простые.

**Генерируем открытый ключ B:**   
Bi = Si \* r mod q  
103 \* 1007 mod 58147 = 45574  
107 \* 1007 mod 58147 = 49602  
211 \* 1007 mod 58147 = 38038  
430 \* 1007 mod 58147 = 25987  
863 \* 1007 mod 58147 = 54996  
1716 \* 1007 mod 58147 = 41777  
3449 \* 1007 mod 58147 = 42528  
6907 \* 1007 mod 58147 = 35974  
13807 \* 1007 mod 58147 = 6754  
27610 \* 1007 mod 58147 = 9481

B = {45574, 49602, 38038, 25987, 54996, 41777, 42528, 35974, 6754, 9481} – откр. ключ

Чтобы **расшифровать**, нужно вычислить а-1 – обратное к а число, такое что а\*а-1(mod n) = 1 (расшир. алг Евклида):  
58147 = 1007 \* 57 + 748   
1007 = 748 \* 1 + 259   
748 = 259 \* 2 + 230   
259 = 230 \* 1 + 29   
230 = 29 \* 7 + 27   
29 = 27 \* 1 + 2   
27 = 2 \* 13 + 1 => обратные преобр:

1 = 27-2\*13 = 27-(29-27)\*13 = 27\*14-29\*13 = (230-29\*7)\*14-29\*13 = 230\*14-29\*111 =   
= 230\*14-(259-230)\*111 = 230\*125-259\*111 = (748-259\*2)\*125-259\*111 = 748\*125-259\*361 =   
= 748\*125-(1007-748)\*361 = 748\*486-1007\*361 = (58147-1007\*57)\*486-1007\*361 =   
58147\*486 + 1007\*(-28063)

a-1 = 58147 – 28063 = ***30084***

2. Найти первообразные корни (если сущ.) чисел (р): 19, 23, 27, 31, 37

19 : {2, 3, 10, 13, 14, 15} + 19n, n≥0  
23 : {5, 7, 10, 11, 14, 15, 17, 19, 20, 21} + 23n, n≥0  
27 первообразных корней нет  
31 : {3, 11, 12, 13, 17, 21, 22, 24} + 31n, n≥0  
37 : {2, 13, 15, 17, 18, 19, 20, 22, 24, 32, 35} + 37n, n≥0

3. Пользователю системы RSA с его собств. ключевыми параметрами n=3337, e=79 передано зашифрованное сообщение, состоящее из 3 блоков: чисел, соотв. порядковым номерам Ваших ФИО. Расшифровать это сообщение (взломав с-му RSA юзера)

Напр, юзер получил блоки шифротекста (Чистякова Юлия Александровна - 25, 32, 01). Надо определить исх. сообщение (числа или буквы исх. сообщения)

кто не может, полегче: ключ. инфа базир на исп-и числа q=47

p\*q = n = 3337, e = 79  
p, q обязательно простые числа, а 3337 раскладывается только на 2 простых числа:

3337 | 47  
71 | 71  
1 |

=> p=47, q=71  
ф = (p-1)\*(q-1) = 46\*70 = 3220

**Найдем d:**  
(d\*e) mod ф = 1  
(d\*79) mod 3220 = 1  
Методом подора находим, что 80501 mod 3220 = 1 (80501 кратно 79)  
 d = 80501 / 79 = 1019

{e;n} – откр. ключ, {d;n} – закр. ключ  
{Ч; Ю; А} --> {25, 32, 01}

исходное:  
251019 mod 3337 = 2894  
321019 mod 3337 = 900  
011019 mod 3337 = 1

4. Пусть в с-ме примен алг шифрования/расшифр Эль-Гамаля. Известны нек. параметры с-мы: p=167, q=5, y=q29 = 55mod p  
Используя указаные и недостающие (выбрать самому) параметры, зашифровать свое имя (в любом языке) в предположении:  
а) первая буква алфавита соотв. числу 0 и т.д.  
б) первая буква алфавита соотв. числу 1  
проанализировать результаты

p=167, q=5, x=29  
y = 529 mod 167 = 55  
Пусть k=5: r = qk mod p = 55 mod 167 = 119  
 m = e\*yk mod p :

а) ю = 31 31\*555 mod 167 = 110  
 л = 12 12\*555 mod 167 = 118  
 и = 9 9\*555 mod 167 = 5  
 я = 32 32\*555 mod 167 = 92

б) ю = 32 32\*555 mod 167 = 92  
 л = 13 13\*555 mod 167 = 100  
 и = 10 10\*555 mod 167 = 154  
 я = 33 33\*555 mod 167 = 74

Проанализировали результаты: mi(б) = mi(а) + 18 mod 167  
где mi(б), mi(а) – i-й символ в алфавита (а), (б) соответсвенно

5. лр 9/6: Сколько попыток нужно сделать, чтобы с вероятностью более 0.5 (0.7, 0.8, 0.9) обнаружить коллизию при длине хеша (l) 64 (128, 256, 512) бит?

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| l,бит | Вероятность | | | |
|  | 0,5 | 0,7 | 0,8 | 0,9 |
| 64 | 5,1\*109 | 6,6\*109 | 7,7\*109 | 9,2\*109 |
| 128 | 2,2\*1019 | 2,9\*1019 | 3,3\*1019 | 4,0\*1019 |
| 256 | 4,0\*1038 | 5,3\*1038 | 6,1\*1038 | 7,3\*1038 |
| 512 | 1,4\*1077 | 1,8\*1077 | 2,1\*1077 | 2,5\*1077 |

m = 2l,

6. лр 9/8: Рассчитать общую длину (L’) хешируемого сообщения после предвар. стадии на основе алгоритма MD5, если объем (L) исх. сообщения составлял: 0, 484, 512, 1000, 2000, 16000 бит. Какова в каждом случае будет длина хеша?

Входное сообщ. начальной длиной L бит расширяется так, что остаются незаполненными всего лишь 64 бита, чтобы итоговая L’ была кратной 512. В указанные 64 бита записывается двоичная длина L.

0 (1 сообщ) --> 512 бит  
484 (1 сообщ) --> 1024 бит  
512 (2 сообщ) --> 1024 бит  
1000 (3 сообщ) --> 1536 бит  
2000 (5 сообщ) --> 2560 бит  
16000 (32 сообщ) --> 16384 бит

Длина хеша для всех случаев будет 128 бит

7. лр 9/9: Входное сообщение (прообраз) состоит из а) имени, б) ФИО.  
Используя представление сообщения в кодах ASCII, представить в табл.форме содержание каждого 32-битного подблока расширенного входного сообщения

а) Пусть прообраз М = “ЮЛЯ”, или в кодах ASCII – это будут десятичные (222-203-223) и соответствующие двоичные (11011110 - 11001011 - 11011111) числа. Как видим, длина L хешируемого сообщения равна 24 битам. Эту длину мы должны расширить до 448 бит, добавив одну «1» и 423 «0». В последнюю часть из 64 бит полученного 512-битного модуля (L’=512) мы запишем справа двоичное представления числа L=24: 11000. В остальные 59 разрядов (из 64) мы впишем «0». После этого полученный расширенный блок делим на 16-ти 32-разрядных подблоков:

11011110110010111101111110000000  
00000000000000000000000000000000  
00000000000000000000000000000000  
00000000000000000000000000000000  
00000000000000000000000000000000  
00000000000000000000000000000000  
00000000000000000000000000000000  
00000000000000000000000000000000  
00000000000000000000000000000000  
00000000000000000000000000000000  
00000000000000000000000000000000  
00000000000000000000000000000000  
00000000000000000000000000000000  
00000000000000000000000000000000  
00000000000000000000000000000000  
00000000000000000000000000011000

б) М = “ЧИСТЯКОВА ЮЛИЯ АЛЕКСАНДРОВНА”, L = 8\*(9+4+13)=208 (10010000)

|  |  |  |
| --- | --- | --- |
| Ч - 10010111 И - 10001000 С - 10010001 Т - 10010010 Я - 10011111 К - 10001010 О - 10001110 В - 10000010 А - 10000000 | Ю - 10011110 Л - 10001011 И - 10001000 Я - 10011111 | А - 10000000 Л - 10001011 Е - 10000101 К - 10001010 С - 10010001 А - 10000000 Н - 10001101 Д - 10000100 Р - 10010000 О - 10001110 В - 10000010 Н - 10001101 А - 10000000 |

10010111100010001001000110010010  
10011111100010101000111010000010  
10000000100111101000101110001000  
10011111100000001000101110000101  
10001010100100011000000010001101  
10000100100100001000111010000010  
10001101100000010000000000000000  
00000000000000000000000000000000  
00000000000000000000000000000000  
00000000000000000000000000000000  
00000000000000000000000000000000  
00000000000000000000000000000000  
00000000000000000000000000000000  
00000000000000000000000000000000  
00000000000000000000000000000000  
00000000000000000000000010010000