ассим. криптография осн. **на решении задач**: (все исп. mod)  
\* разлож на сомнож (зад. факторизации) RSA  
\* вычисл. дискрет. log в конечном поле Эль-Гамаль  
\* вычисл. операции над точками эллипт. кривой

**Осн. теорема арифметики:** всякое нат. N, кроме 1, можно предст на произв. простых множ.  
**Задача дискр. лог:** для целых a>1, b<n найти логарифм х, если сущ. : ax = b (mod n)  
 x = logAb  
**Китайская теорема об остатках:** если разложение N на простые множ. это p1\*..\*Pt (нек. простые числа м. встречаться неск. раз), то система уравнений (x mod pi) = ai, где i=1,2…t  
имеет един. решение: х, меньшее N  
Т.е., число (меньшее, чем произведение неск. простых чисел) однозначно опред. своими вычетами по модулю от этих простых чисел

**Алгоритм RSA:**

+ проще понять и реализовать

**Генерация компонентов ключа (n,e,d\*):** //d\* - тайна  
\* случ. большие простые p, q (лучше равной длины == сложнее найти сомнож)  
\* n=pq  
\* выбир. e, вз-простой с (p-1)(q-1) = ф(n)  
\* счит. d, d-1 = e(mod ф(n)) по обр.Евклида ed = 1 mod (ф(n))  
=> (e,n) – откр. ключ; (d,n) – закр.ключ

**Зашифрование:** ci = (mi)e mod n //mi,ci - блоки  
**Расшифрование:** mi = (ci)d mod n

**Алгоритм Эль-Гамаля:**

\* для заш/расш данных  
\* для формир цифр. подписи  
\* для согласования общ. ключа  
\* для проверки пароля, док-ва идентичности сообщ…

**Отличие от RSA:**  
1) генерация ключ. инфы и число компонент ключа  
2) к. блоку mi соотв. 2 блока ci (в RSA 1:1)  
3) при зашифр исп. число (k), кот. почти не связано с ключом + приним разные значения при зашифр разных блоков mi  
4) вероятностный характер шифр (k разные знач)

**Генерация ключ. инфы (p,g,x\*,y):**\* выбир простое p  
\* выбир g<p – первообразный корень числа p  
\* выбир х<p  
\* вычисл. y, y = gXmod p

**Зашифрование:** 2 блока ci ai = gkmod p, bi = (yk \*mi) mod p  
**Расшифрование:**  mi = (bi \*(ai)p-x-1) mod p

**Первообразный корень по модулю p** – число, его степени (gi, 1≤ i ≤ p-1) дают все возможные по модулю p остатки, кот. взаимно просты с p  
**Пр:** p=5, остатки 2i mod 5 - 2, 4, 3, 1

**Криптостокойсть:** для больших p кол-во всех остатков (p-1) больше == найти x очень трудно  
т.к. при использ. разных степений (ai=aX) решение будет равномерно распред. от 0 до p-1  
Если для зашифрования блоков m1, m2 исп. одинаковые k, то для c1=(a1,b1), c2=(a1,b2) вып. соотношение b1(b2)-1 = m1(m2)-1 == легко вычисл. m2, если известно m1

**ЗАДАНИЕ:**

1. табл/граф форма зависимости времени вычисл y=aXmod n,  
от **а** (1,2 числа 5-35), **х** (5-10 простых равномерно-распред. в 103-10100), **n** (чила, в двоич из 1024 и 2048 бит)

2. заш/расш Эль-Гамаля + RSA текст. доков  
\* опр. время  
\* ключ сгенер. самому или библ OpenSSL

**Вопросы для контроля и самоконтроля:**

1. Охарактеризовать алгоритмы RSA и Эль-Гамаля. Для каких целей они могут применяться?

*RSA:* + проще понять и реализовать  
*Эль-Гамаля:*  
\* для заш/расш данных  
\* для формир цифр. подписи  
\* для согласования общ. ключа  
\* для проверки пароля, док-ва идентичности сообщ…  
*Отличия:*  
1) генерация ключ. инфы и число компонент ключа  
2) к. блоку mi соотв. 2 блока ci (в RSA 1:1)  
3) при зашифр исп. число (k), кот. почти не связано с ключом + приним разные значения при зашифр разных блоков mi  
4) вероятностный характер шифр (k разные знач)

2. На чем основана криптостойкость алгоритмов RSA и Эль-Гамаля?

*Эль-Гамаль*: вероятностный характер шифр (k разные знач)  
*RSA*: трудность разложения на множ. больих чисел

3. Что такое первообразный корень?

число, его степени (gi, 1≤ i ≤ p-1) дают все возмож. по модулю p остатки, кот. взаимно просты с p  
**Пр:** p=5, остатки 2i mod 5 - 2, 4, 3, 1