Lucrare de laborator nr. 5
КРИПТОГРАФИЯ С ОТКРЫТЫМ КЛЮЧОМ

Задание 1. Изучайте учебно-методические материалы, размещенные на ELSE.

Задание 2.1. Используя платформу *wolframalpha.com* или приложение *Wolfram Mathematica*, сгенерируйте ключи, зашифруйте и расшифруйте сообщение

m = Имя Фамилия,

применяя алгоритм RSA.
Значение *n* должно быть не менее 2048 бит.

Задание 2.2. Используя платформу *wolframalpha.com* или приложение *Wolfram Mathematica*, сгенерируйте ключи, зашифруйте и расшифруйте сообщение

m = Имя Фамилия,

применяя алгоритм Эль-Гамаля. Значения *p* и *генератора* заданы ниже.

Задание 3. Используя платформу *wolframalpha.com* или приложение *Wolfram Mathematica*, выполнить обмен ключами Диффи-Хелмана между Алисой и Бобом, которые используют алгоритм AES с 256-битным ключом.
Секретные числа *a* и *b* должны быть выбраны случайным образом в соответствии с требованиями алгоритма. Значения *p* и *генератора* заданы ниже.

Примечания:
1. Для заданий 2.1 и 2.2 используйте десятичное числовое представление сообщения, получив их через шестнадцатеричное символьное представление в соответствии с кодировкой ASCII. Для удобства в конвертации вы можете воспользоваться страницей https://www.rapidtables.com/convert/number/hex-to-decimal.html.
2. Для заданий 2.2 и 3 используйте значегия
p=32317006071311007300153513477825163362488057133489075174588434139269806834136210002792056362640164685458556357935330816928829023080573472625273554742461245741026202527916572972862706300325263428213145766931414223654220941111348629991657478268034230553086349050635557712219187890332729569696129743856241741236237225197346402691855797767976823014625397933058015226858730761197532436467475855460715043896844940366130497697812854295958659597567051283852132784468522925504568272879113720098931873959143374175837826000278034973198552060607533234122603254684088120031105907484281003994966956119696956248629032338072839127039,
care are 2048 biți și generatorul *g*=2.

Отчет должен сопровождаться подробными комментариями по всем шагам алгоритмов!!!

Полезные функции в *Wolfram*:

- ***Prime*[*n*]** – *возвращает n-е простое число из списка простых чисел (n ограничено);*
- ***RandomPrime*[{i_{min}, i_{max}}]** – *возвращает псевдослучайное простое число между* i_{min} и i_{max} *;*
- ***RandomInteger*[i_{max}]** – *возвращает псевдослучайное целое число между* ***0*** и i_{max} *;*
- ***Mod[a, n]*** – *возвращает остаток от деления* ***a*** *на* ***n****;*
- ***PoerMod[a, b, n]*** – *возвращает остаток от деления* a^b *на* ***n****;*
- ***FactorInteger [n]*** – *возвращает список простых множителей числа* ***n*** *вместе с их показателями;*
- ***IntegerDigits[n, b]*** – *возвращает список цифр целого числа* ***n*** *в системе счисления по основанию* ***b****;*
- ***Length[lst]*** – *возвращает длину списка* ***lst****;*