

Белорусский государственный университет информатики и
радиоэлектроники

Кафедра информатики

Лабораторная работа № 4

Асимметричная криптография. Алгоритм Эль-Гамала.

Выполнила студентка гр. 653502: Сулима М.Ф.

Проверил ассистент КИ: Артемьев В. С.

Минск, 2019

Введение

Схема Эль-Гамала (Elgamal) — криптосистема с открытым ключом, основанная на трудности вычисления дискретных логарифмов в конечном поле. Криптосистема включает в себя алгоритм шифрования и алгоритм цифровой подписи. Схема Эль-Гамала лежит в основе бывших стандартов электронной цифровой подписи в США (DSA) и России (ГОСТ Р 34.10-94).

Схема была предложена Тахером Эль-Гамалем в 1985 году. Эль-Гамаль разработал один из вариантов алгоритма Диффи-Хеллмана. Он усовершенствовал систему Диффи-Хеллмана и получил два алгоритма, которые использовались для шифрования и для обеспечения аутентификации. В отличие от RSA алгоритм Эль-Гамала не был запатентован и, поэтому, стал более дешевой альтернативой, так как не требовалась оплата взносов за лицензию. Считается, что алгоритм попадает под действие патента Диффи-Хеллмана.

В рамках лабораторной работы необходимо реализовать программные средства шифрования и дешифрования при помощи алгоритма Эль-Гамала.

Блок-схема алгоритма

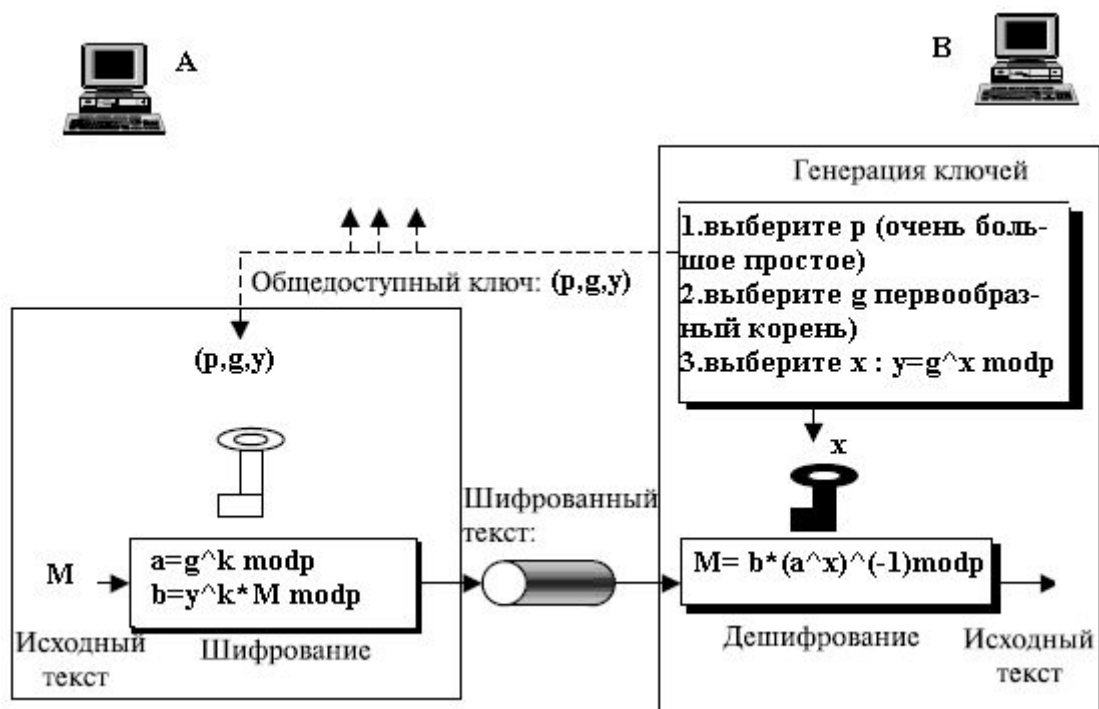


Рис.1. Схема алгоритма

Пример работы программы

```
enc text : 30002924797123969616499752785101062467231620023293349939311377914825441822344 59693936569003248286514393226781336842302669729423397117784637207927311601138
50760778604923159052275102601766991399682790484475803532572043434179919214677 160531125076860113099697282873063269957847032297798957906220970176379139416
14893886947729831825316944052888144252556303641718157409701525582289714962121 25045809029681704582382708964524716119802893167452602828131238119113078231783
72706969054380482237999331487973017306957795505601570437822655779917159074409 39987183521259276926535636968206008871674257423205691513928818735846890899770
24756026362688956255005429349718727378352633126787550961948466234928522512510 39633046544268070675814249132195636946317201457335529760207474890882123131737
56233283184964142318519258821177588354825935970268722910171131934618480789584 48337701111547010725073890991361009518954089062832407651459183166896521369610
75261577034784466576673143534072351367397111044627463919287682061117759975334 62653385905185369441102927373241107344589193576823765176886772237268014215019
76250062064535593989793162866194752673785019287017448398622579387195484744093 62002636223337007897855124136592145920763052125032391231183413337141858243079
75713335904426586509114618721394316693679920218816855024484862663818943072584 58336956335267306866430021824498221780132052448716174218874714215908484965224
2001792279248595807532375844345644881090942428539759084185819874201496790922 18881611029300263820097658201865905733233246397418471402554774724602220080027
12875787126400135116088200972248101243288125259133285407356153790339416253834 3069473297523006670662043346935648542421340944260521083551217999538688665035
2969504410118911497664623327724195631392289045863713624109655817885009876003 67200012827458739646312121677673651506826635823742338437611388306720076956499
8221288014462803538714079017447481735445631355596571004314007275836218049635 753861100354024140094489926071860336634530192603771833706635254505110936087
11120196396068743719044808452456875974860528295252283349253719542870970051264 39963996528924319641055031362328142713634377084469674067138657320765433834913
74216334520231137507447383751480196311170470414934070572296109620271805445810 11510243714618798411497180981264042539083966840364207639356953856318207358645
70439931301348433095921993946605843015337475148329316023436019275877542682744 49547716024845735987656194555212452798408163966602573338007051522667879879995
43591051150207699022557943701538465207313883564193847164422516037968998477210 15025990277857092314765551829671992716330230825891038610897708763530531081263
24692249771764197442022122675021535433398032573440444628431753541792123591394 74827758168965572869796067449282787498971524805550450446500322331441013195333
51217705583522229883559501042194370689476931148679003048199334745061646000987 15124334010747623795875583378520987669376247620058815587515166067230284157846
24950921530809329781451084145480253164533351434126765428760195735261412383831 16539407998199972062127617600826546928888890255916965239911516786601271977800
dec text: qwerty12345678ytrwq
```

Рис.2. Пример работы

Код программы

```
def generate_keys(confidence=32):
    p = find_prime(256, confidence)
    g = pow(find_primitive_root(p), 2, p)
    x = random.randint(2, p - 1)
    y = pow(g, x, p)
    publicKey = {'p': p, 'g': g, 'y': y}
    privateKey = {'p': p, 'x': x}
    return privateKey, publicKey

def encrypt(key, plainText):
    z = bytearray(plainText, 'utf-8')
    cipher_pairs = []
    for i in z:
        k = random.randint(2, key['p'] - 1)
        a = pow(key['g'], k, key['p'])
        b = (i * pow(key['y'], k, key['p'])) % key['p']
        cipher_pairs.append([a, b])
    encryptedStr = ""
    for pair in cipher_pairs:
        encryptedStr += str(pair[0]) + ' ' + str(pair[1]) + ' '
    return encryptedStr

def decrypt(key, cipher):
    plaintext = []
    cipherArray = cipher.split()
    if len(cipherArray) % 2 != 0:
        return
    for i in range(0, len(cipherArray), 2):
        a = int(cipherArray[i])
        b = int(cipherArray[i + 1])
        s = pow(a, key['x'], key['p'])
        plain = (b * pow(s, key['p'] - 2, key['p'])) % key['p']
        plaintext.append(plain)
    decryptedText = bytearray(plaintext).decode('utf-8')
    return decryptedText
```

Вывод

В настоящее время криптосистемы с открытым ключом считаются наиболее перспективными. К ним относится и схема Эль-Гамала, криптостойкость которой основана на вычислительной сложности проблемы дискретного логарифмирования, где по известным p , g и y требуется вычислить x , удовлетворяющий сравнению:

$$y \equiv g^x \pmod{p}$$

В ходе написания лабораторной работы были изучены алгоритмы шифрования и дешифрования Эль-Гамала, а также написаны их программные реализации.