Queen Mary
University of London

MTH6115 Cryptography

Assignment 8 Not for handing in (2011)

This work should not be handed in; it is for you to practise to help understand various concepts of the course. There will be no tutorials for this, but you are welcome to visit me during my normal tutorial hours (in my office) and my office hours (in term-time).

Remember: *As usual, even if you work in groups, make sure you understand everything yourself.*

1 My El-Gamal public key is $(p, g, h) = (619, 233, 601)$. Encrypt the message $x = 164$ for sending to me (there are several solutions to this). You receive the message $(581, 201)$ sent with the above key. Decrypt it, given that my private key has $a = 110$.

2 Exercise in RSA encoding. Write down a string consisting of your student number, followed by a colon and a space, followed by your name with usual capitalisation and spacing. Do not use accented letters and the like. An example might be:

`076543219: Dr John N. Bray.`

(Exclude the full stop at the end.) Convert this into a sequence of ASCII codes $a_0, a_1, \ldots$ (which would be $48, 55, 54, 53, 52, 51, 50, 49, 57, 58, 32, 68, 114, 32, 74, 111, 104, 110, 32, 78, 46, 32, 66, 114, 97, 121$ here), then convert this into the single integer $x := \sum_{i=0}^{\ell-1} a_i 128^i$, where ℓ is the length of your string. (You should restrict this length ℓ to 100 characters.)

My RSA key is (N, e), where N and e are given below. Encrypt your plaintext x using this RSA key and send to a friend.

$$N = 126447594075563763027326274282772882722428604978062528079676-\\ 298622739059982482461797318514511477315032435558276091835255-\\ 422255057661816635933545721467893686391991967228242600266949-\\ 303350074745881730260148645240581372980198012869027720363140-\\ 327829644261849976207851736400662722559822890469251288224851.$$

$$e = 138386450095043880008115747714161986973022306731830970471 25-\\ 111363606871575840435398147336398075095986534185193242785092-\\ 776410861009955579814320769115386703276498933178269369096563-\\ 531748071793375276307663017037796882234575655753515663714912-\\ 408073921636061753550825347084102454290150247845478894876565.$$

My decrypt key is d, which is given below. If you have received a message from your friend, decrypt it using this key, then recover the original message, which you should communicate to your friend.

$$d = 176848016117908307182972645531588514222904074766258646586583-\\ 0039099239611859488034045083815859573960348677987235751001 70-\\ 7494969905479729195186171185983549778943729012265686458047 49-\\ 9091674379663425869236824734770818524346599212970727217212 62-\\ 9957986848600270413978278804129480665702235640928725777607 97.$$

Use the known values of N, d, e to factorise N, which is the product of two distinct odd primes. (Do not use this key for any information you want to be kept secure; I have compromised its security by publishing the value of d.)

3 The following are primes q such that $p := \frac{q-1}{2}$ is also prime. With a minimum of calculation, find primitive roots modulo q for each of these values of q. The values of q are 503, 1319, 2099, 3467, 4079, 61799663, 62924879 and 89694083.

4 Let the integers $a_1, \ldots, a_{11}$ be $1, 3, 13, 26, 52, 108, 221, 445, 896, 1792, 3584$, and let $b = 2135$. Determine (the unique) $e_i \in \{0, 1\}$ such that $b = e_1a_1 + \cdots + e_{11}a_{11}$.

5 Let the integers $a_1, \ldots, a_{11}$ be 1371, 6855, 70, 2882, 315, 7485, 4072, 8179, 1382, 5506, 6934, and let $b = 11872$. Determine (the unique) $e_i \in \{0, 1\}$ such that $b = e_1a_1 + \cdots + e_{11}a_{11}$.