

EE2302 Foundations of Information and Data Engineering

Assignment 5

Due: 5:00 pm, Oct 10 (**Wed**)

Full Mark: 18 points

You can hand in your assignment during the tutorial sessions (Mon or Wed). I will also put a collection box next to the door of my office (G6354, YEUNG) during the following periods:

- Oct 10 (Wed): 2:00 – 3:00 pm
- Oct 10 (Wed): 4:00 – 5:00 pm

Solution will be posted to Canvas on Wednesday evening for you to prepare for the quiz.

1. (6 points) For each part, find a value of x that solves the given simultaneous congruences.
 - a) $x \equiv 3 \pmod{37}$ and $x \equiv 5 \pmod{87}$
 - b) $x \equiv 5 \pmod{7}$, $x \equiv 2 \pmod{12}$ and $x \equiv 8 \pmod{13}$
2. (6 points) Consider the use of RSA cipher. The public key of Bob is $N = 55$ and $e = 3$.
 - a) Alice wants to send the message “HELLO” to Bob. Translate the message into its numeric equivalent (i.e. $A = 1, B = 2, \dots$).
 - b) Encrypt the message in (a) letter by letter. (In practice, individual letters of the alphabet are grouped together in blocks during encryption so that deciphering cannot be accomplished through knowledge of frequency patterns of letters or words.)
 - c) Suppose Bob receives a message from Claire. The ciphertext of the message is 08 05 15. Decrypt it and translate the result into letters of the alphabet to discover the message.

3. (6 points) This question requires the use of SageMath (or other math software).

Consider the RSA cipher with the following public key:

$N = 38485385893612647530529565399136160386558570363459$

$e = 12036041725135809493242715057143070093942766266573$

- a) Find the value of d for decryption.

- This can be efficiently done by computer because the value of N in this question is not too large. In Sage, the function `inverse_mod(x, y)` gives the multiplicative inverse of x modulo y .

- b) Decrypt the ciphertext shown below (which consists of four letters) and translate the result into letters of the alphabet to discover the message.

3167406316726521398545793438566521165012474274617

1

26638565906273003780154505098111173562745814216350

14566383257015530139469069221369279753772335716877

- In Sage, the function `power_mod(x, y, z)` returns $x^y \bmod z$.

Exploratory Exercise (**Optional; not to be handed in**)

4. This question aims to demonstrate that an RSA cipher can be easily broken if the two primes are not chosen carefully. Consider the following public key:

$N = 357177030895805008781319266876641103581839678151495135129133067010127$

$e = 278958316326567585064962258326769977220638526280473113990619654480829$

- a) Factorize N using Pollard's attack.

- You are encouraged to learn this method from books or the Internet so as to deepen your understanding of RSA.

- b) Find the value of d for decryption.

- c) Decrypt the ciphertext shown below (which consists of four letters) and translate the result into letters of the alphabet to discover the message.

113064473595933840468586734675005367858578684317668774505229820418325

260035994288728320669528342074180612357059196752620848700734251673334

40378293680253925650969959071520886320817907928810947026202852533894

245886810806739778794194015749870344083424800876374311167612988144799