Εργασία #2

Οδηγίες.

1. Αν λύσετε όλα τα θέματα σωστά θα έχετε **1.5 μονάδες** στον βαθμό της τελικής εξέτασης με την **προϋπόθεση να γράψετε τουλάχιστον 5.**
2. Δείτε το Readme.txt
3. Ο κώδικας σε python (γενικά ισχύουν τα ίδια με την προηγούμενη εργασία).
4. Επίσης, δηλώστε τα ονοματα σας στο google doc για την εργασία ή προσθέστε ένα δικό σας θέμα. Το google_doc θα το βρείτε στο Readme.txt.
5. Κώδικας python για συνεχή κλάσματα https://github.com/AristotleUniversity/python_scripts/blob/master/cont_fractions.py (άσκηση 6 (β))
6. Deadline : 5 μέρες πριν την εξέταση του μαθήματος

ΘΕΜΑΤΑ

Θέμα 1. (20%) Να απαντήσετε σύντομα στις παρακάτω ερωτήσεις :
(i) Περιγράψτε το πρωτόκολλο ανταλλαγής κλειδιών Diffie-Hellman.
(ii) Δώστε τον ορισμό ενός κρυπτοσυστήματος δημοσίου κλειδιού.
(iii) Δώστε τον ορισμό της Trapdoor function (TDF).
(iv) Ποια λύση προτείνετε για να αποφύγουμε την *Man-in-the-Middle-Attack* στον Diffie-Hellman;
(v) Δώστε τον ορισμό της εντροπίας κατά Shannon. Ποια είναι η εντροπία που προκύπτει από το στρίψιμο ενός νομίσματος;
(vi) Περιγράψτε επιθέσεις και απειλές που μπορούν να γίνουν σε μια ψηφιακή υπογραφή.
(vii) Αν p=463,q=547 και e=101, αποκρυπτογραφήστε με το RSA-textbook το κείμενο c=236784.
(viii) Αποδείξτε ότι η υπογραφή RSA (αν δεν κατακερματίσω το μήνυμα) πλαστογραφείται (ολικά) με επίθεση επιλεγμένου κειμένου.
(ix) Δικαιολογήστε γιατί δεν πρέπει να χρησιμοποιώ δύο φορές το ίδιο εφήμερο κλειδί στο σύστημα υπογραφής DSA.
(x) Αν N=pq (p,q πρώτοι), αποδείξτε την ισότητα $\varphi(N)=N-(p+q)+1$.

Θέμα 2. (10%) (i) Υπολογίστε τον gcd(126048,5050) και βρείτε τους συντελεστές Bezout.

(ii) Υπολογίστε το αντίστροφο στοιχείο του 809 στο $\mathbf{Z}_{1001}$.

(iii) Υπολογίστε το υπόλοιπο του 2^{100} με το 101 (χωρίς την χρήση του παρακάτω αλγορίθμου).

(iv) Υλοποιήστε τον παρακάτω αλγόριθμο **fast(),** σε όποια γλώσσα προγραμματισμού θέλετε (ο αλγόριθμος αυτός είναι παραλλάγη αυτού που έχω στις σημειώσεις)

Input. a, g, N

Output. $a^g \bmod N$

1. $g = (g_n g_{n-1} \cdots g_0)_2$
2. $x \leftarrow a,\ \delta \leftarrow 1$
3. for i=0 to n do

   if $g_i = 1$ then $\delta \leftarrow \delta x \bmod N$; end if

   $x \leftarrow x^2 \bmod N$

   end do

   return δ

Κατόπιν υπολογίστε τις δυνάμεις $2^{1234567} \bmod 12345,\ 130^{7654321} \bmod 567$.

Θέμα 3. (10%) Έστω **n = 4003997** και **e = 379** και **φ(n) = 3999996**.

(i) Βρείτε τον μυστικό εκθέτη **d**.

(ii) Βρείτε πρώτους **p,q** τέτοιους ώστε **n = pq**.
Υποδ. Για το (ii) χρησιμοποιήστε την ισότητα N+1-φ(N)=p+q. Επομένως γνωρίζετε το γινόμενο και το άθροισμα των p,q , υπολογίστε τα p,q.

Θέμα 4. (10%) Λύστε το σύστημα των γραμμικών ισοδυναμιών (Κινέζικο Θεώρημα Υπολοίπων)

$$x \equiv 9 \pmod{17}$$
$$x \equiv 9 \pmod{12}$$
$$x \equiv 13 \pmod{19}$$

Βρείτε την λύση που ικανοποιεί 0<x<1000.

Θέμα 5. (10%) (text RSA) Δίνεται το δημόσιο κλειδί **(N,e)=(11413,19)**. Βρείτε το ιδιωτικό κλειδί και κατόπιν αποκρυπτογραφήστε το μήνυμα

```
C=(3203,909,3143,5255,5343,3203,909,9958,5278,5343,995
8,5278,4674,909,9958,792,909,4132,3143,9958,3203,5343,
792,3143,4443)
```

Υποθέστε, ότι τα γράμματα στο αρχικό μήνυμα m, αναπαρίστανται από τις ASCII τιμές τους (δουλέψτε block by block το C).
Υποδ. Παραγοντοποιήστε το N, κατόπιν υπολογίστε το φ(N)…θα χρειαστεί και η συνάρτηση fast().

Θέμα 6. **(i) (10%)** Βρείτε το συνεχές κλάσμα του ρητού αριθμού (χωρίς κώδικα!)

$$\frac{123454}{546542}$$

(ii) (20%) (text RSA) Αν

```
(N,e)=(194749497518847283,50736902528669041)
```

και το κρυπτογραφημένο κείμενο

```
C=[4740626319269350 9,5106517820117222 3,3026056523512870 4,8238596333440426 8
8169156663927929,4740626319269350 9,1782759773366964 42,1344342958948038 06
1121115718355123 07,1193911517610508 82,3026056523512870 4,8238596333440426 8
1344342958948038 06,4740626319269350 9,4581532097256020 2,1746322293120412 48
3026056523512870 4,4740626319269350 9,1193911517610508 82,5720807776658530 6
1344342958948038 06,4740626319269350 9,1193911517610508 82,4740626319269350 9
1121115718355123 07,5288285102607250 7,1193911517610508 82,5720807776658530 6
1193911517610508 82,1121115718355123 07,8169156663927929,1344342958948038 06
5720807776658530 6,4740626319269350 9,1855821052750509 32,1746322293120412 48
1344342958948038 06,8238596333440426 8,1725653863934436 24,1063565018935464 01
8169156663927929,4740626319269350 9,1036105972061081 6,1344342958948038 06
1193911517610508 82,1725653863934436 24,4740626319269350 9,8169156663927929
5288285102607250 7,1193911517610508 82,8169156663927929,4740626319269350 9
4581532097256020 2,1746322293120412 48,3026056523512870 4,4740626319269350 9
5288285102607250 7,1193911517610508 82,1115234082124818 79,1344342958948038 06
4740626319269350 9,1121115718355123 07,5288285102607250 7,1193911517610508 82
5720807776658530 6,1193911517610508 82,1121115718355123 07,8169156663927929
1344342958948038 06,5720807776658530 6]
```

έχει προκύψει από το textbook-**RSA** (block by block).
Εφαρμόστε την επίθεση του *Wiener* για να βρείτε το κλειδί **d**.
Υποθέτουμε ότι στο αρχικό κείμενο **m** κάθε χαρακτήρας έχει αντικατασταθεί από την ASCII τιμή του. Για τον υπολογισμό των δυνάμεων $x_i^d \bmod N$, χρησιμοποιείστε την συνάρτηση **fast().** Τέλος, βρείτε το αρχικό μήνυμα **m**.

Θέμα 7. (10%) Έστω p=5,q=11 και το κρυπτογραφημένο μήνυμα c=14 έχει προκύψει από την εφαρμογή της TDF του Rabin σε ένα μήνυμα m. Βρείτε το αρχικό μήνυμα m αν γνωρίζετε ότι το m<20.

Θέμα 8. (10%) Το κείμενο m έχει κρυπτογραφηθεί με την χρήση του textbook RSA και με δημόσια κλειδιά (N[i],e[i]) : {(391,3),(55,3),(87,3)} και πήραμε αντίστοιχα τα c[1]=208, c[2]=38, c[3]=32. Να βρεθεί το m.
Τι πιστεύετε ότι πρέπει να προσέχει κάποιος όταν κρυπτογραφεί ένα μήνυμα m με τον ίδιο δημόσιο εκθέτη; Μπορείτε να διατυπώσετε μια γενική επίθεση στο textbook RSA;
Υποδ. Λύστε το σύστημα
x=208(mod391), x=38(mod55), x=32 (mod 87).
Ψάχνετε έναν αριθμό m : m^3=c[i]modN[i] (i=1,2,3)

Θέμα 9. (10%) Έστω $f(x) = x^2 + x - 1354363$. Διαλέξτε 100 τυχαίους ακέραιους αριθμούς x, στο διάστημα $[1,10^4]$ και εφαρμόστε το Τεστ του Fermat στους αριθμούς $|f(x)|$.
(α) Τι παρατηρείται;

(β) Υπάρχει πολυώνυμο του Z, που για κάθε ακέραια τιμή να μας δίνει πρώτο αριθμό; (δικαιολογήστε την απάντηση σας, είτε δίνοντας κάποια αναφόρα, είτε αποδεικνύοντας κάποιο θεώρημα).

Θέμα 10. (α) **(8%)** Να κατασκευάσετε με την μέθοδο Fermat έναν πρώτο αριθμό με 1024 bits.

(β) **(12%)** Να λύσετε την εξίσωση $3^x = \alpha$, όπου $\alpha \in Z_{43}^*$, με τις μεθόδους Shanks και Pollard-ρ, για α=2,4,5.

Θέμα 11. (10%) Με χρήση του προγράμματος GPG δημιουργήστε ένα PGP-πιστοποιητικό και κάνοντας χρήση του δικού μου δημοσίου κλειδιού (δείτε το Readme.txt), στείλτε μου ένα κρυπτογραφημένο μήνυμα με χρήση του ηλ.ταχυδρομείου. Μην ξεχάσετε να μου στείλετε και το δημόσιο κλείδι σας σε ξεχωριστό μήνυμα (εννοείται χωρίς κρυπτογράφηση). Σε περίπτωση που είστε ομάδα, κάθε άτομο της ομάδας να κάνει την εργασία ξεχωριστά. Ως απάντηση στείλτε μου την ημερομηνία αποστολής του μηνυματός σας.

Καλή Επιτυχία!