Εργασία #1

Οδηγίες.

1. Η 1η εργασία είναι προαιρετική. Εφόσον ασχοληθείτε, πρέπει να την επιστρέψετε με τα ονόματα και τους αριθμούς μητρώου σας μέχρι **13 Απριλίου**. Μπορείτε να τη στείλετε στο e-mail : *drazioti at csd.auth.gr*
2. Η κάθε ομάδα να αποτελείται από **3** άτομα το πολύ. Φυσικά, μπορείτε να δουλέψετε και ατομικά.
3. Αν τα λύσετε όλα σωστά θα έχετε **+1 μονάδα** στο βαθμό της τελικής εξέτασης με την **προϋπόθεση** να γράψετε **τουλάχιστον 5**.
4. Η εργασία να είναι γραμμένη με το σύστημα **Latex**. debatable
5. Σε ασκήσεις που ζητάται κώδικας, να σταλεί και αυτός (σε **python**).
6. Μην αναζητήσετε έτοιμο κώδικα στο internet! Αλλά αν αυτο συμβεί τουλάχιστον να είστε έντιμοι και να δώσετε τα απαραίτητα credits!

ΘΕΜΑΤΑ

Theory

Θέμα 1. (10%) Να απαντήσετε σύντομα στις παρακάτω ερωτήσεις:
(i) Διατυπώστε την αρχή του Kerchoff και γράψτε ποιος ο λόγος που διατυπώθηκε.
(ii) Δώστε τον ορισμό της τέλειας ασφάλειας ενός κρυπτοσυστήματος. Υπάρχουν συστήματα με τέλεια ασφάλεια;
(iii)
(iv) Το OTP παραμένει ασφαλές αν χρησιμοποιήσουμε το ίδιο κλειδί δύο φορές;
(v) Περιγράψτε την κατάσταση λειτουργίας ECB σε ένα συμμετρικό κρυπτοσύστημα τμήματος.

Practical: Implementation with Python

Θέμα 2. (10%) Υλοποιήστε τον RC4. Χρησιμοποιώντας το κλειδί MATRIX κρυπτογραφήστε το μήνυμα

Never send a human to do a machine s job

Θέμα 3. (15%) (Vigenere) Να αποκρυπτογραφήσετε το κείμενο που βρίσκεται στο text file vigenere.txt
Να γραφεί αναλυτικά η μεθοδολογία.
(όταν το αποκρυπτογραφήσετε, προσπαθήστε να βάλετε τα σωστά σημεία στίξης).

With brute force?

Θέμα 4. (5%) Το παρακάτω κείμενο κρυπτογραφήθηκε με το σύστημα της μετατόπισηςς (επίσης υπάρχει στο file vigenere.txt).

ΟΚΗΘΜΦΔΖΘΓΟΘΧΥΚΧΣΦΘΜΦΜΧΓΟΣΨΧΚΠΦΧΘΖΚΠ

Θέμα 5. (10%) Κάνοντας χρήση της βιβλιοθήκης pycrpto (https://pypi.python.org/pypi/pycrypto) εξετάστε αν ισχύει το avalanche effect στον AES. Αναλυτικότερα, φτιάξτε αρκετά ζευγάρια (>30) μηνυμάτων (m1,m2) που να διαφέρουν σε ένα bit. Μελετήστε σε πόσα bit διαφέρουν τα αντίστοιχα κρυπτομηνύματα.
Αναλυτικότερα

```
#το key πρέπει να είναι 16 byte. Διαλέξτε όποιο κλειδί θέλετε.
from Crypto.Cipher import AES
key='something'
obj=AES.new(key,AES.MODE_ECB)
# κρυπτογράφηση #
message="something"
ciphertext1=obj.encrypt(message)  # το message να είναι 16 byte.
ciphertext2=ciphertext1.encode('hex')
ciphertext=bin(int(ciphertext2, 16))[2:]  # το κρυπτογραφημένο μήνυμα μετατρέπεται σε δυαδικά ψηφία.
...
```

Θέμα 6. (10%) Τα γράμματα του Αγγλικού αλφαβήτου έχουν αριθμηθεί όπως παρακάτω.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	0

Ένα μήνυμα με **n** γράμματα έχει κρυπτογραφηθεί με ένα κλειδί που αποτελείται από **n** γράμματα. Ο αριθμός του κάθε γράμματος προστίθεται στον αντίστοιχο αριθμό του κλειδιού και το αποτέλεσμα ανάγεται ***mod 26*** και αντικαθίσταται από τα γράμματα του πίνακα. Αν το κλειδί περιέχει μόνο τα γράμματα **K,E,Y,** αποκρυπτογραφήστε το κείμενο, **χωρίς** χρήση κώδικα. Απαντήσεις που θα έχουν brute force **δεν θα χρεωθούν** τις μονάδες της άσκησης.

AJZBPMDLHYDBTSMFDXTQJ

Θέμα 7. (15%) Το αρχείο `test_zip.zip` (υπάρχει στον pilea) είναι κλειδωμένο με κωδικό. Ο στοχός αυτής της άσκησης είναι να τον βρείτε κάνοντας χρήση της βιβλιοθήκης `zipfile` της python. Σε αυτήν την άσκηση θα χρειαστείτε ένα λεξικό το οποίο και σας επισυνάπτω στον pilea με το όνομα english.txt.

Η εντολή που θα ελέγχει κάθε φορά τον υποψήφιο κωδικό από το english.txt είναι :

```
>> zFile=zipfile.ZipFile("test_zip.zip") # αυτό θα γίνεί μία φορα στην αρχή του κώδικα σας, και
>> zFile.extractall(pwd=password)  # αυτή θα εκτελείτε σε μία conditional συνθήκη εώς ότου βρει τον κωδικό
```

Όταν ο κωδικός σας δεν είναι σωστός, οπότε και θα έχετε ένα μήνυμα λάθους, το οποίο πρέπει με κάποιο τρόπο να αγνοηθεί και το πρόγραμμα να συνεχίζει στην επόμενη γραμμή του english.txt (το english.txt δεν είναι λεξικό με την έννοια ότι περιέχει όλους του δυνατους συναδυασμους λέξεων,συμβόλων, κλ.π. Απλά περιέχει κάποιες *συνηθισμένες* λέξεις).

Θέμα 8. (15%) Στόχος αυτής της άσκησης είναι να αποκτήσετε πρόσβαση στον server sage.csd.auth.gr (όχι root!). Έχει έρθει στα χέρια σας (με κάποιο τρόπο...) ένα τμήμα του αρχείου `/etc/shadow` (το επισυνάπτω στον pilea ως `password.txt`). Επίσης γνωρίζετε ότι ο κωδικός είναι εξαψήφιος και αποτελείται μόνο από αριθμούς. Εφόσον τον βρείτε κάντε *ssh* στον server χρησιμοποιώντας το account που βρήκατε. Τέλος, γράψτε το όνομα σας και το αεμ στο αρχείο `my_name` (βρίσκεται στο home folder του user. Χρησιμοποιείστε nano my_name για να εισάγετε το ονομα και το αεμ σας και κατοπιν ctrl+x και Y για να το σώσετε).
(Υποδ. - Θα χρησιμοποιειθεί η συνάρτηση

```
import crypt
crypt.crypt(password,"$6$salt$")
```

Όπου το salt θα το δείτε από το αρχείο `password.txt`

- Το (encrypted) password στην άσκηση αυτή το έχετε.Πρέπει να θέσετε password =" αυτο που σας δίνω "
- Δεν χρειάζεστε λεξικό (αλλά nested loops που να βρίσκουν όλες τις εξάδες ακεραιών μεταξύ 0 και 9.
- Για ssh από windows θα χρειαστείτε τον ssh-client putty)

Θέμα 9. (i) (5%) Περιγράψτε ένα κρυπτοσύστημα τμήματος εκτός του DES, 3DES και AES.
(ii) (5%) Περιγράψτε συνοπτικά την αρχή λειτουργίας του ψηφιακού νομίσματος Bitcoin.

Καλή Επιτυχία!