CIS 3362 Homework #7: Elliptic Curves and Breaking DES

Homework Protocol: To be done in pairs

Due via Webcourses: Friday, December 1, 2023 11:59 pm

Working Pairs

Many students do NOT have to do this assignment because they've already done the community service. Please pair up with one student in the class (who did not do the community service) and tell me in person who you are working with. I'll add the two of you to a group just for this homework assignment. If you never tell me you are in a group and you didn't do the community service, then I will add you to a group by yourself so that you can submit the assignment.

The deadline to get added to a group is November 29th at 11:30 am (beginning of class).

Assignment Part I: Get 16 bits of a DES key

A DES Key has 56 bits. Given the usual computing resources the average individual has, it's infeasible for them to break DES within 2 weeks by trying all 2^{56} keys. But, it would be feasible to try upto 2^{40} keys. (Code will take some time to run though, after it's written.) To that end, part I of this assignment will be to uncover 16 of the bits of the DES key used in Part II.

Recall that a DES key is specified with 64 bits labeled k_1 through k_{64} where k_8, k_{16}, …, k_{64} are odd parity bits for each byte.

In this part of the assignment, you'll discover the bits

k_1, k_2, k_3, k_4, k_9, k_{10}, k_{11}, k_{12}, k_{17}, k_{18}, k_{19}, k_{20}, k_{25}, k_{26}, k_{27}, and k_{28}.

In particular, if you follow the directions given, you'll generate an integer in between 0 and 65,535 ($2^{16} - 1$). Represent this integer in the regular unsigned binary notation assigning k_1 to the most significant bit, k_2 to the second most significant bit, etc. k_{28} to the least significant bit.

How to retrieve 16 bits of the DES key

Alice and Bob are using the Diffie-Hellman Key Exchange with Elliptic Curves to share a secret key. The curve they are using is:

$E_{65543}(12271, 36523)$.

Thus, their prime number is 65543. Their value of a = 12271. Their value of b = 36523.

The generator point they are using is:

(34555, 18773).

Using this generator point, Alice has sent to Bob the following point, which you have intercepted:

(26035, 25302)

In return, Bob has sent Alice the following point, which you have also intercepted:

(19563, 2605)

Once Bob and Alice respectively receive these points, they multiply them by their respective secret keys to yield a shared secret point (x, y).

The 16 bits you are to recover for the use in part 2 as specified above are stored in the value of x in this shared secret point.

Note: You may use any of my ECC code only to help with this portion of the assignment.

Assignment Part II: Break DES

The ciphertext on the next page was encrypted via DES (my DES.java code). The encoding technique used was Radix-64. The details of its use are described below. Note: There is an easier way of determining, without physically looking at a potential decryption for valid English text, if it's valid or not. Discovering this will greatly speed up the decryption process. I recommend discovering this first before ever running your brute force code.

Protocol used to carry out DES

The original plaintext message was written using valid Radix-64 characters only. A list of these characters and their conversions to a 6-bit integer can be found online: https://en.wikipedia.org/wiki/Base64.

The original plaintext file contained exactly 10 Radix-64 characters per line. For each line, these characters were converted to their binary equivalent, yielding 60 bits. Then, four 0s were added to the end of this, creating 64 bits.

These 64 bits are the input to DES.

Then, the 64 output bits from DES were padded with two more 0s, creating a ciphertext of 66 bits.

These 66 bits were then converted back to 11 Radix-64 characters. Thus, the given ciphertext file consists of 11 Radix-64 characters per line.

The ciphertext to break is included on the next page and a separate file will be provided with it also.

To help you with the assignment, you may use the implementation of DES shown in class that is posted on the course web page.

What To Submit

1. A Document detailing the work that you did. (Descriptions in English with references to code used/written.)

    a. This description must include your strategy for finding the ECC shared key.
    b. This description must include the full shared point and either Alice of Bob's secret key.
    c. This description must include your strategy for using the 16 bits given in part 1 so that only 40 bits are brute forced.
    d. This description should include the DES key (if found), including parity bits.
    e. This description should include the decrypted plaintext (if found) in Radix-64.
    f. This description should include a nicely formatted version of the plaintext.

2. Code you used to help with both parts of the assignment.

3. Any other supporting files/documentation you think will be helpful to the graders.

Note: Part A is worth 25 points, Part B is worth 100 points.

Ciphertext to break

```
F87iFrYsVSE
GsxrwtC4OPc
Tb9xCT4MB3Y
98diwPjrjmE
1t/N6TRhnek
hX5MRJdEj1I
OS6QRxkiE0Q
bb9cAR57SUQ
pJN8KXr5XjI
f2Y5yUcb+zM
5LV3Q7KXXPw
9GIKbsAhDLM
S9SN29h90II
SSyemyQ+/pE
79Whu0bcvhU
wpSv+yr05Lg
Qvtv4g1Ym8A
x6Y3WC7Ag0E
TeAE08/Oskc
f0BjkHphMCk
jQQCz8eGYsA
MI9LZShh44c
G5smdoTH6ao
/DXiLU3KTfc
GVE0IT7thlI
cS8hav5FDEA
eML10IgSQNY
wyJHuhGAMs8
6m1OGjITgp0
0dEr2zuYvBM
otB9STvxWbM
1nEOpPLj0ag
FdtKGUYZzPA
ElbBBvOKO5Y
dDNTNFqFw5I
ZAtrJGJ0vJw
VgGNFkIPWpA
RrJfIjxXIPw
P3DpAAm6Afg
Bq8Tkge9GCc
tUGbf2jiRSs
duOlMLwgZTM
jlI5fTZz0Go
Mry50AE9TF4
EuRpziJX7Qc
SfmIwRGVGqQ
HK46lvJlhGE
```