Aniruddha Jafa, Paul Kurian, Vidur Singh May 2, 2019

CS-302 Problem Set 5

Collaborators: *Aniruddha Jafa, Paul Kurian, Vidur Singh*

Problem 5-0

Code for SHA 3 is submitted along with this doc.

101 was treated as a decimal and then converted to binary (confirmed by TA). Then the shift index was calculated as a mod (128) number (TA had asked us to look at this code again). Implemented the algorithm found on wikipedia and the function given in the hunt itself.

The answer was a 56 bit number: 11111001100010011110101100001111111101001111000000011001

Problem 5-1

We decrypted the cipher text with DES with the above mentioned 56-bit number as the key, IV as suggested in the prompt. With that we found the following plain text:

golookforaclue/in712/ithappenstobe/inonelessthantwo

We realized this referred to 712 in SH1 ("inonelessthantwo"), where we found a note, which told us the answer was the "very second clue". After some thought we realized this might mean it was the very second cryptic clue given in the course, which we found in PSET 2. We knew the answer to that clue was "shannon" (one of our teammates had solved this when PSET 2 was first given). On entering this, we got to the next level.

Problem 5-2

From the clue we saw on the SH1 712 door – "For the level after, do your readings that is the protocol (drop the s, all small)" – we went through Piazza for extra syllabus readings (we also tried the appendices in the slides, but this wasn't getting us anywhere). We found a reading posted by Barun on "Kerberos" which we realized could be the key to the DES decryption algorithm after "dropping the s" because only DES required such a 7 letter key. Also, the wikipedia page on Kerberos mentioned both AES and DES (which helped orient us in this direction), and we had written decryption code only for DES, for PSET 2. This whole process (the "Kerberos hint) was by far the most time consuming. The hint on piazza ("the garbled circuit part is not necessary to move on to the next level.") also helped, although we couldn't figure out how the second piazza hint ("secondly, hashing algorithms are familiar") fit in. We didn't know which IV to us, so we tried using the same IV as what was used in the previous round. Luckily this worked!

We hence decrypted the text which led us to "look for a red pole between 2 academic blocks". After searching for a bit with our phone flashlights at 2am (and presumably weirding out a bunch of onlookers), we found a clue on the fire hydrant near the science block and the new academic block which told us to look for the "most important bits", which we took to understand as the most significant bits. We thus copied the most significant bit from each byte in the ciphertext given in this round, and that was the answer.

Problem 5-3

We decrypted the cipher text using the Vigenere decryption code we had written for PSet 1. We tried Vigenere because the ciphertext ("snhffr cvfgr") seemed to fit such a encryption scheme, and "Vigenere" was also a French name (in the prompt "Abientot, et merci pour tous les poissons!" was a French phrase). Upon decrypting we got "faussepiste" which means "wrong track" in English. After some thinking we realized that this literally meant we were on the wrong track and we read the next line which told us to provide feedback to our TA Barun. We remembered that Barun had shared a link on Piazza for providing feedback sometime ago, and went to the Piazza link. Once we filled that (Barun, please read it, we meant everything we said on it), we found the answer to proceed to the next level.

Problem 5-4

After removing the punctuation and numbers from the given ciphertext we ran it through the same Vigenere decryption algorithm from Pset 1 used in the previous level (again, we used Vignere since the ciphertext seemed to be in a form amenable to such an encryption scheme), which gave "ending" as the likely key, and a big block of text talking about garbage. However, hidden in the block of text was the clue which suggested we should look in some SH drawer for a french perfume. To find which hostel number, we pasted the ciphertext on crypti.com, with "ending" as the key, and got the decryption intact with numbers etc (recall that earlier we had removed numbers and special characters so that we could use our pset 1 code).

We found a crossword in one of the drawers of the SH1 common room. The crossword had a clue regarding french perfume. We looked at the corresponding row, and typed the answer to finish the last level. The answer was "descent". Thus we finished the hunt (although didn't manage to learn what the bonus hidden question was).