ECS608U/ECS760P Security Coursework

Na Yao

February 2017

When many time pad is used for encryption, it becomes very easy to crack the ciphers. Below are eleven hex-encoded ciphertexts that are the result of encrypting eleven plaintexts with a stream cipher, all with the same stream cipher key. Your goal is to decrypt the last ciphertext, and submit the secret message within it.

1. 1B 11 4D 11 0C 09 00 01 00 15 4F 47 1E 0A 0E 1F 00 11 15 41 0D 54 4F 12 48 07 52 12 02 04 00 0A 00 15 01 44 53 1A 0E 1A 44 44 1A 07 4E 54 0E 54 4F 0C 1D 55 17 4E 03 08 0C 11 53 41 0C 11 54 4E 0F 03 16 06 00 06 1A 56 08 55 16 18 00 03 00 52 18

2. 1D 1C 45 54 11 19 0A 07 4F 02 4F 0B 52 12 00 07 00 0A 04 0C 09 44 4F 07 46 16 17 13 56 2E 17 0B 42 11 1D 4F 00 54 07 1C 0B 4D 55 37 52 11 0A 4B 4F 18 0B 54 0D 01 09 02 0E 1C 53 54 0A 10 54 46 0F 07 1C 17 49 0E 06 53 4D 01 0B 1A 45 11 4F 48 16 15 05 0B 00 00 12 05 41 06 0B 00 0B 1A 15 00 09 14 49 2D 0F 00 16

3. 1D 1C 45 54 25 0A 11 12 00 24 4E 04 00 1C 11 00 49 0B 0B 41 3F 54 0E 08 44 03 00 05 56 0C 01 59 41 54 1C 59 1E 19 04 1A 16 49 16 50 4B 11 16 00 0E 19 15 4F 17 07 11 05 04 45 15 4F 10 55 00 48 0F 55 16 1A 43 13 0A 50 19 1C 0C 06 00 1B 09 00 16 18 04 0D 10 52 1A 1E 49 17 4F 44 0E 01 13

4. 0C 1A 43 06 18 1B 11 1A 4F 0F 00 0E 01 45 15 1C 45 44 15 13 03 43 0A 15 53 42 1D 07 56 00 1C 1A 4F 10 06 4E 14 54 00 4E 09 45 06 03 41 13 0A 00 06 1B 52 53 10 0D 0D 4D 08 45 04 41 1B 55 15 53 4A 01 1C 54 48 08 17 45 4D 1C 17 1B 00 17 00 4E 07 11 0F 1A 17

5. 1D 1C 45 06 04 4B 04 01 45 41 54 10 1D 45 15 0D 50 01 16 41 03 46 4F 03 4E 01 00 18 06 11 1B 16 4E 54 0E 4C 14 1B 13 07 10 48 18 50 53 0D 02 4D 0A 01 00 49 06 4E 00 03 0A 17 0A 50 16 1C 1B 4E 4A

14 1D 10 00 00 00 59 00 18 06 1C 52 1D 0C 00 16 1A 02 1C 1D 50 01 19 4F 1A

6. 1D 1C 45 54 37 02 02 16 4E 04 52 02 52 06 08 04 48 01 17 41 05 53 4F 07 00 0F 17 15 1E 0A 16 59 4F 12 4F 45 1D 17 13 17 14 54 1C 1E 47 54 0E 4C 1F 1D 13 42 00 1A 0C 0E 49 11 16 58 16 55 16 59 4A 00 00 1D 4E 06 53 41 4D 06 06 1A 49 11 1C 00 1C 12 41 0A 0D 46 13 15 52 11 01 54 4F 36 13 45 15 13 1B 45 0D 0D 03

7. 1A 00 52 1B 0F 0C 45 17 49 06 49 13 13 09 41 07 49 03 0B 00 18 55 1D 03 53 42 13 13 13 45 13 17 00 11 1C 53 16 1A 15 07 05 4C 55 02 45 05 1A 49 1D 10 1F 45 0B 1A 45 0B 06 17 53 53 07 16 01 52 0F 55 00 0D 53 15 16 4D 1E

8. 0C 02 45 1A 41 1F 0D 16 00 12 4D 06 1E 09 04 07 54 44 15 04 1E 53 00 08 00 01 13 0F 56 06 1A 18 4E 13 0A 00 07 1C 04 4E 07 4F 00 02 53 11 4F 4F 09 55 06 48 00 4E 03 18 1D 10 01 45

9. 1D 1C 45 54 22 0A 00 00 41 13 00 04 1B 15 09 11 52 44 04 0D 1F 4F 4F 0D 4E 0D 05 0F 56 04 01 59 41 54 1C 48 1A 12 15 4E 07 49 05 18 45 06 4F 49 1C 55 1D 4E 00 4E 0A 0B 49 11 1B 45 42 06 1D 4D 1A 19 16 07 54 41 15 4F 1F 18 10 48 4F 12 4F 45 1D 17 13 17 14 54 1C 1F 4E

10. 1B 27 61 54 08 18 45 1E 41 05 45 47 1D 03 41 00 48 01 45 08 02 49 1B 0F 41 0E 52 0D 13 11 06 1C 52 07 4F 4F 15 54 15 06 01 00 06 05 52 1A 0E 4D 0A 06 52 4F 03 4E 37 02 07 45 21 49 14 10 07 54 4A 34 17 1D 00 32 1B 41 00 1C 11 48 41 1A 0B 00 3F 11 0E 00 05 52 11 50 61 10 03 45 02 14 1C

11. 0B 18 4F 17 0A 4B 06 1A 50 09 45 15 01 45 15 15 4B 01 45 00 4C 4E 1A 0B 42 07 00 41 19 03 52 1B 49 00 1C 00 12 1A 05 4E 01 4E 16 02 59 04 1B 00 1B 1D 17 4D 45 0F 16 4D 08 45 00 49 0C 12 18 45 4A 00 1D 1D 54 41 12 4E 09 55 13 09 44 10 06 4E 14 54 15 06 01 00 05 1C 41 1D 01 54 0A 0D 06 00 15 1D 49 11 06 05 07

Hint: Both the messages and key are in English. The feature of XOR a letter with a space producing the same letter of opposite case can be used for this problem.

Requirements You need to write a little Java programme to calculate the XORs of ciphertexts. Submit a report giving the results of XORs in your answer and explaining how you decrypted the messages using XOR results.

Marking criteria: 20% for the correctness of the Java code, 30% for the correctness of the decryption results, and 50% for the explanation of the full decryption process and all necessary interim results.