Bitcoin, Blockchain and Cryptoassets
Exercise Set 1

In this exercise set you will get a chance to train how to convert between different numeral systems, try to break a symmetric cipher and use the RSA algorithm to encrypt and decrypt a message.

Keep in mind that solving this exercise set is voluntary and UNGRADED. The solutions are either shared already or will be in due time.

Exercise 1

This first exercise aims at making you familiar with the conversion between different numeral systems.

Exercise 1.1

a) Convert the binary number $(\texttt{10110101})_{B=2}$ into a decimal number.

b) Conver the decimal number $(93)_{B=10}$ into a binary number.

Exercise 1.2

a) Convert the binary number $(\texttt{10110101})_{B=2}$ into a hexadecimal (with basis $B = 16$).

b) Convert the hexadecimal $(9c3a)_{B=16}$ into a binary number.

Exercise 2

The following (English) text was encrypted with the monoalphabetic substitution cipher:

RQL IFMXAXQKNY XQKFFLYZL NH K ZJLKR MOOMJRGYNRD RM ZKNY OJKXRNXKF LPOLJNLYXL TGJNYZ DMGJ HRGTNLH KYT RM UMJA MY K FKJZLJ OJMVLXR RMZLRQLJ UNRQ K XMEOKYD.
RQL HRGTLYR RLKEH TLHNZY K HMFGRNMY MY RQL IKHNH MC K OJKXRNXL-MJNLYRLT OJMIFLE TLHXJNORNMY. KXXMEOKYNLT ID XMKXQLH KYT LPOLJRH, RQLD ZM RQJMGZQ RQL HRLOH NY XJLKRNYZ K XMYXLOR NYXFGTNYZ K OJMRMRDOL. RQNH KNEH KR HRJLYZRQLYNYZ RQLNJ RLKEUMJA, MJZKYNHKRNMYKF KYT OJLHLYRKRNMY HANFFH, KH ULFF KH NEOJMWNYZ RNEL EKYKZLELYR KYT OJMIFLEHMFWNYZ XMEOLRLYXL. CGJRQLJEMJL, RQL XQKFFLYZL MCCLJH K GYNBGL XQKYXL RM YLRUMJA UNRQ XMEOKYNLH KYT LPOLJRH KH ULFF KH HRGTLYRH UQM KJL NYRLJLHRLT NY RQL HKEL RMONXH.

Decrypt it using frequency analysis and by exploiting the relations between letters. (Hint: Use frequency analysis only to decipher the three most frequent letters. Also, there are online tools which can help you with finding the relative frequencies of the letters[1]).

[1] E.g. `https://www.mtholyoke.edu/courses/quenell/s2003/ma139/js/count.html`

Exercise 3

In this exercise we use the RSA algorithm covered in the lecture on asymmetric cryptography to create a private and public key and send an encrypted message along the lines of the example in the lecture. We use the parameters $p = 11$, $q = 23$ and $e = 7$ to encipher the message L.

Exercise 3.1

Compute the number N and convert the message $M = L$ using the ASCII table into a decimal number (!). Thereafter encrypt this decimal number to receive the encrypted message C.[2]

Exercise 3.2

Compute the number $\phi(N)$ and derive the private key k_p, which will be used to decrypt the message C.

Hint: To find the multiplicative inverse in modulo-calculations we have to use the Euklidean Algorithm. There are several online tools which you can use, instead of doing this by hand[3].

Exercise 3.3

Decrypt the encrypted message C using the private key k_p and check the result with the original message $M = L$.

[2]Conventional calculators might not be able to handle numbers of this size well. We recommend to use the online modulo calculator of https://planetcalc.com/8326/.

[3]A simple tool would be the inverse calculator by https://planetcalc.com/3311/. To derive the private key (k_p) in the RSA example in the lecture on asymmetric cryptography you would have to insert 7 und "Integer" and 160 under "Modulo". The result is the private key k_p. Use the analogous procedure in this exercise.

Exercise 4

The following (blue text) is encrypted with the same cipher alphabet as used in Exercise 2. Punctuation marks are not encrypted. Furthermore you will need the RSA algorithm with the parameters from Exercise 3, the ASCII conversion table from the lecture on symmetric cryptography, and you must be able to convert between different numeral systems, as covered in Exercise 1. Decrypting this text will give you all the informations you need to come up with the solution.

RQL ALD UMJT NH RQL 01001100010000010101001101010100 UMJT MY OKZL 192 NY RQL LYZFNHQ INRXMNY UQNRLOKOLJ MY INRXMNY.MJZ OFGH RQL TLXNEKF JLOJLHLYRKRNMY MC RQL QLPKTLXNEKF 4b.

To verify if you have found the correct solution, concatenate (no spaces) the word and the number, compute its SHA256 hash value using an online hash calculator and compare it to the hexadecimal string below. Example: If your solution is "bitcoin" and "21" you would have to compute the SHA256 of "bitcoin21". Make sure you write the word in lowercase letters and add no spaces. As you have learned in the lecture, even the smallest change in the input will lead to an entirely different hash value. The SHA256 hash value of the correct solution is:

75324da9af9da0e9ea77abc4a0c46afffd7e6f80080652e149fc19f26a10b97f