Information (and Network) Security, Coursework 1 submission deadline 10/Nov/2019

Submission guidelines

1. Please submit a single pdf file.
2. In your submission please avoid handwriting.
3. Please accompany all of your answers with short explanations.
4. In this module an *algorithm* means just a sequence of steps. You can use a plain English, no need to use a pseudocode nor a programming language. That said, however, your description must be *effective*. In other words, your description must be sufficiently detailed for somebody else to apply your algorithm and to obtain the correct answer.

1 Operations with binary numbers (15 points)

1.1 From binary to decimal (5 points)

Convert the binary number 1011101 into the decimal form.

1.2 Bitwise logical operations (10 points)

First of all, let us make our notation more in line with the standard math. The operations OR,AND, and NOT we considered in the class are usually denoted by $\vee, \wedge, \neg$, respectively. That is, instead of A OR B, A AND B, and NOT A, we respectively, write $A \vee B$, $A \wedge B$ and $\neg A$.

With this in mind compute the result of bitwise operation $\neg((\neg A) \vee (\neg B))$, where $A = 01010101$ and $B = 10101111$.

Hint: The above operation might be looking a littlle bit formidabe but in fact, by properly opening the brackets, it can be replaced by a simple bitwise operation. This can be done by so called **De-Morgan's laws** and remembering that $\neg(\neg A) = A$. I recommend you first to try this simplification and only afterwards to apply this operation to the simplified vectors.

Needless to say that you are free to ignore the above recommendation and to apply the specified bitwise operation directly to the vectors stated.

2 Some number theory (20 points)

2.1 Greatest common divisors (5 points)

Determine the greatest common divisors of the following pairs of numbers

- 15 and 120.
- 120 and 120.
- 72 and 84.

2.2 Decomposition into prime numbers (5 points)

Decompose number 144 into prime numbers.

2.3 Modular multiplication (10 points)

Let $A = 12345678912345$ and $B = 135792222$. Determine whether $A * B$ equals 0, 1, or 2 modulo 3 **without performing the actual multiplication of these numbers**.

Describe the step of your reasoning. **Without this description, marks will not be awarded.**

Hint: Use the following 'multiplication table' modulo 3.

- $0(mod3) * i(mod3) = 0(mod3)$ for each $i \in \{0, 1, 2\}$
- $1(mod3) * i(mod3) = i(mod3)$ for each $i \in \{0, 1, 2\}$
- $2(mod3) * 2(mod3) = 1(mod3)$.

3 Vigenere cipher (10 points)

Encode the text $informationsecurity$ using the Vigenere cipher with the keyword run.

4 Cipher with a permutation-based key (25 points)

Consider the following permutation F of $\{1, 2, 3\}$: $F(1) = 2$, $F(2) = 3$ and $F(3) = 1$. This permutation suggests the following encoding of a 3-letter word: the first letter of the word goes to the second place, the second goes to the third place and the third letter goes to the first place. For example, the world run wll be encoded as nru.

Suppose we have a longer text whose length is a multiple of 3. Then the encoding is done as follows.

1. The text is divided into 3-letter blocks.

2. Each of the blocks is encoded as specified above.

3. The encoded blocks are joined back together.

For example, the text *ilovemath* is encoded as follows.

1. The 3-letter blocks of this text are *ilo*, *vem*, and, *ath*.

2. The respective encodings of these blocks are *oil*, *mve* and *hat*.

3. The resulting encoding of the whole text is *oilmvehat*.

4.1 Encoding a particular text (5 points)

Using the cipher defined above, encode the text $noinformationsecurity$.

4.2 Decoding of the cipher (10 points)

Design a decoding algorithm for the above cipher. Demonstrate the work of this algorithm by decoding the text obtained as a result of your solution of the previous question.

4.3 Generalization of the cipher (10 points)

Generalize the idea of the above cipher by descrbing the encoding algorithm for an arbitrary permutation of set $\{1, \ldots, n\}$.

5 Feistel encoding

Consider the encryption system described in the previous question.

For example, consider the word 010101. Partition the word into blocks of length 3 that are 010 and 101. Then do the 'forward shift' to each of these blocks as specified by the permutation in the explanatory part of the previous question. The first block will become 001 and the second block will become 110. Finally join the blocks to obtain 001110.

Please answer the following questions.

1. **15 marks.** Describe a Feistel encryption system whose input is the above encryption algorithm (recall that Feistel encryption is a generic method that uses another encryption system as input).

2. **15 marks.** Using the description as in the previous question, encrypt the following plaintext 011110100001.