2014-AT-01-EN Secret Message

0 ----	I: ----	II: ----	III: hard	IV: medium	
☒ ALG	☒ INF	☐ STRUC	☐ PUZ	☐ SOC	☐ USE

Answer Type: Multiple Choice Graphics are: not used in this task

Body

Tom and Andrew heard about a cypher algorithm at school.
They want to try it out to share their math homework-solutions.
The algorithm is based on a square of numbers from 0 to 9 each row and column and an additional column including characters of their forenames (**TOM_ANDREW**).
They need to choose and share a **password** consisting characters of the first column only (the password is **WONDER_TOMATO**).

To encrypt a message you have to write it under the password so you can link each password character to a message digit.
For each pair of characters and digits you will find a cipher-coded-digit in the square. The characters locate the row and the digits locate the column of the cipher-digit.

T	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
O	**9**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
M	**8**	**9**	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
_	**7**	**8**	**9**	**0**	**1**	**2**	**3**	**4**	**5**	**6**
A	**6**	**7**	**8**	**9**	**0**	**1**	**2**	**3**	**4**	**5**
N	**5**	**6**	**7**	**8**	**9**	**0**	**1**	**2**	**3**	**4**
D	**4**	**5**	**6**	**7**	**8**	**9**	**0**	**1**	**2**	**3**
R	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**0**	**1**	**2**
E	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**0**	**1**
W	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**0**

For example:

Password	**W**	**O**	**N**	**D**	**E**	**R**	**_**	**T**	**O**	**M**	**A**	**T**	**O**
example-message	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**0**	**1**	**2**	**3**
example-cipher-code	**2**	**1**	**8**	**8**	**7**	**9**	**4**	**8**	**8**	**8**	**7**	**2**	**2**

Tom has solved a math-task and got **299792458** (m/s... speed of light) as a result.
Now he's waiting for Andrews encrypted code to compare.

Question

How does Andrews encrypted message must look like to ratify Toms result?

Answer

PW:	**W**	**O**	**N**	**D**	**E**	**R**	**_**	**T**	**O**
A)	**3**	**8**	**4**	**0**	**1**	**5**	**1**	**5**	**7**
B)	**3**	**8**	**4**	**1**	**1**	**5**	**1**	**5**	**7**
C)	**3**	**8**	**4**	**1**	**1**	**5**	**4**	**5**	**7**
D)	**2**	**9**	**9**	**7**	**9**	**2**	**4**	**5**	**8**

Explanation

Answer B is correct. A is wrong because the fourth digit is 1 (row D, column 7).
C is wrong because the seventh digit is 1 (row _, column 4).
Answer D is wrong because it's the plain-text of the message.

It's informatics

The task is a lite version of a Vigenère-cipher. It is an old but powerful poly-alphabetic symmetric-key cipher which is based on substitution.
Given that the following conditions are complied:
1) the message is not longer than the password
2) the password was chosen by chance
3) the password was used the first time
Then the cypher is provably unbreakable (one-time-pad).

Keywords

Vigenère-cipher, one-time-pad, symmetric-key algorithm, poly-alphabetic cipher

Websites

http://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher
http://en.wikipedia.org/wiki/Polyalphabetic_cipher
http://en.wikipedia.org/wiki/One-time_pad
http://sharkysoft.com/misc/vigenere/
(online tool to de/encrypt by using vigenere-cipher)
http://www.mygeocachingprofile.com/codebreaker.vigenerecipher.aspx
(online tool to break vigenere cipher-code)

Internal Use

Wording

Pairs of characters and digits leads to a cipher-coded-digit (for example: (W,2) → 3 or (O,9) → 8).
A cipher-algorithm is the code of practice to de/encrypt a message.

Comments

Roman Ledinsky, 2014-01-26, reworked version, simplified description.

Files

2014-AT-01-EN.odt (this file)

Authorship

Roman Ledinsky, 2013-11-10, Initial version, inspired by work done by Denise Hackner.
Roman Ledinsky, roman.ledinsky@gmail.com, Austria
Denise Hackner, Austria

License