



## Problem 8. «Scientists»

Two young cryptographers and very curious students Alice and Bob studied different cryptosystems and attacks on them. At the same time they were very interested in biographies of famous scientists and found out one interesting **property** that can be used in cryptosystems. They choose three pair of scientists:

**Charles Darwin** and **Michael Faraday**,  
**Werner Heisenberg** and **Johannes Kepler**,  
**Hans Christian Orsted** and **Mikhail Lomonosov**.

Alice and Bob choose a cryptosystem and an attack they would like to study. They constructed three sets of parameters for the cryptosystem: one set according to each pair of scientists. Then Alice choose a phrase consisting of 18 English letters (spaces were omitted) and divided it into three parts of 6 letters. She represented each part as a hexadecimal number using ASCII code. Alice encrypted the first part by the cryptosystem for each set of parameters, then the same actions she made for the second and the third parts. Finally, Alice got the following three groups of three ciphertexts (in hexadecimal notation):

	Part 1			Part 2			Part 3		
Set of parameters 1	2512	1F5A	0079	B494	222D	3E1C	275E	B751	4FDB
Set of parameters 2	3D0D	6812	0443	5111	5BFD	9398	0815	6223	2698
Set of parameters 3	1EDC	4856	8CE2	9C18	2A32	B9AB	9A1C	AD5C	25D7

and asked Bob to decrypt it using the attack! Bob successfully read the secret phrase. Could you

- find the property like Alice and Bob,
- understand what is the cryptosystem and the attack chosen,
- decrypt the ciphertext by applying this attack?

\*What word should be added at the beginning of the decrypted text according to the famous words of Mikhail Lomonosov?