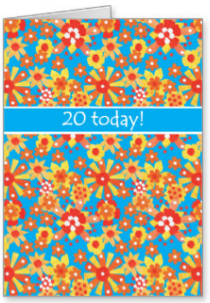
Problem 7. «*Palindrome* cipher»

The company *Palindrome* had been using the block cipher `DES` to encrypt its documents for 12 years since the foundation until its engineers took a decision to use the block cipher `Blowfish` in addition to `DES`. It was in 2005 year. So, up to now all its documents are encrypted by `DES` and then the result is also encrypted by `Blowfish`. The ciphering is conducted in EBC mode. Both ciphers `DES` and `Blowfish` have the same key and block lengths equal to 64 bits. The descriptions of these ciphers can be found here: DES and Blowfish.

As a result of information leakage, that occurred during the celebration of the anniversary of the company, the text of a greeting card leaked to the Internet. The text of the greeting card was

```
Dear colleagues! Congratulations for our wonderful journey of 20 years
of success and we hope the same for the future also!
```



And the ciphertext of that greeting card was

$C =$ `83c100497b13525e fc8d3201d58ab9ed f6820425912ce184`
`23034db7b4408629 4df36ca87ad39f4a 99277e6f1e217dfd`
`f2eab13d1161e849 0fe72e9b98fc1e8a 0aa5680e3b4022cb`
`4e44c8745afae37f bd5d6d49292bd1b2 9386f2f383061bfd`
`ae8fca32e6745687 565d353f3bbb1204 aa79742f7ab55fb1`
`123e6cf37fbad6fe`

Could you decrypt the following ciphertext that was intercepted in the company network few weeks ago:

$C =$ `cf414505b7d3aee3 36f48ae753ec799c fb49aaea17fa2a38 2992ed164e9622aa`
`0b64549dad59a803 0b93be9baf9339e6 fe9780d39168bdff 10d77405d1b51a6a`
`5475ddf991ef3ad9 85a6c0c451b75da5 aa4c59ec0c40af09 852b70cebeb127b9`
`43c362dccbebf21e dbb2b086aba67212 1c92e2f327a03b05 b1affd236d8e0f9c`
`62386237b27597b4 cbe8ec78b07f4ce6`

It is known that an encryption 128-bit key is changed dynamically every day according to certain rules and it is always a sequence of 128 bits where each of 16 bytes is given by ASCII codes of figures from `0` to `9`. The first 64 bits form a `DES` key and the other 64 bits form a `Blowfish` key.

see the next page

Here we present some technical information of the company encryption. Below you can find examples of test vectors for combination of both ciphers `DES` and `Blowfish`. They are given as 64-bit integers $b_{63}b_{62}\dots b_0$ in hexadecimal notation.

plaintext	`DES` key	`Blowfish` key	ciphertext
0000000000000000	0000000000000000	0000000000000000	561543527d054ad0
0000000000000000	0000000000000000	ffffffffffffffff	df27adaec8337f57
0000000000000000	ffffffffffffffff	0000000000000000	11148646af0d82e9
ffffffffffffffff	0000000000000000	ffffffffffffffff	18708bdc3837046f
6c6f632072616544	3837363534333231	3132333435363738	72e66b26309de78c

To form 64-bit integer $b_{63}b_{62}\dots b_0$ each consequent 8 symbols of an original text (or key) are transformed into their ASCII codes and little-endian order of bytes is used.

For example, let us encrypt the message `Dear colleagues!` using the keys `12345678` and `87654321` for `DES` and `Blowfish` correspondingly. We divide it into two blocks of 8 symbols `Dear col` and `leagues!` and encrypt them separately:

$$\texttt{Dear col} \to P_1 = \texttt{6c6f632072616544} \to \texttt{DES} \to T_1 = \texttt{cb32b921efe674e5} \to \to \texttt{Blowfish} \to C_1 = \texttt{72e66b26309de78c}$$

$$\texttt{leagues!} \to P_2 = \texttt{217365756761656c} \to \texttt{DES} \to T_2 = \texttt{f3d9c5f0cf2e9e8f} \to \to \texttt{Blowfish} \to C_2 = \texttt{2d9f9fd83b15ae75}$$

Thus, the ciphertext is `72e66b26309de78c 2d9f9fd83b15ae75`.