

BREAKING COMBINATION CIPHERS

We are moving in on the target, below is a final communication. We believe it was encrypted with autokey, followed by a columnar transposition, and finally a Vigenère cipher.

Fortunately, we believe that one of the keys for the cipher was sent publicly via ElGamal encryption. In particular, we believe that

- The modulus is $n = 59053979$
- The generator is $x = 2$
- We have public data $x^a = 2^a = 4581422$
- and $x^b = 2^b = 19981752$
- and $m \cdot (x^a)^b = m \cdot x^{ab} = 53460947$

Find the message m , turn it back into text, and use it as one of the passphrases. We believe the other passphrases can be obtained in other ways.

Here is the ciphertext:

```
GQZT NCZX TKKN MKBO TLGS IINK NTIX PSOZ CEVZ QJFZ ODVG FDSC GXAE XGLW TRCN VASP
LXTV PLDC DZVO GMNE WFQL RQOM IOLM HWTB AXZG JTKU NGPY EFOV QGCI MJBQ BFAC ZTXC
      UGYF HBNU IV
```