**Problem 1** Symmetric encryption with a deck of cards. Alice shuttles a deck of cards and deals it all out to herself and Bob (each of them gets half of the 52 cards). They do not share any keys. Alice now wishes to send a secret message $M$ to Bob by showing something (probably very very long) publicly. Eavesdropper Eve is listening in: she can see everything Alice shows, but Eve can’t see the cards.

Suppose we want to achieve perfect secrecy; that is, Eve has no information at all about what is $M$. What is the maximum number of bits $M$ can be in this scheme.

**Problem 2** The following two keys enhancements to DES were proposed in order to increase the complexity of finding the keys by exhaustive search. Let us denote them as:

\[
\begin{align*}
DES_{X_{k,k_1}}(M) &= DES_k(M) \oplus k_1, \\
DES_{Y_{k,k_1}}(M) &= DES_k(M \oplus k_1)
\end{align*}
\]

The key length is $|k| = 56$ and $|k_1| = 64$ ($k_1$ is 64 bits because the block size for DES is 64 bits. Show that both these proposals do not increase the complexity of breaking the cryptosystem using brute-force key search. That is, the number of DES encryptions/decryptions is still in the order of $2^{56}$. You can assume that you can have a moderate number of plaintext-ciphertext pairs.