1. This English phrase has been encrypted with a Shift Cipher (26-letter alphabet). What does it say?

QEFPZFMEBOFPSBOVTBXH

Can you classify your attack type?

2. We are trying to break a variable-strength secret key encryption system (e.g. SSLv3). Exhaustive key search through the key-space is the only available method of breaking the cipher. A standard PC CPU + motherboard costing 400 EUR can check about 15 million keys per second. We wish to have a solution within 30 days. How much will such a setup cost (excluding labor etc) for the following effective key sizes?

- a) "Low-grade" encryption: 40-bit key-space.
- b) "Export-grade" encryption: 56-bit key-space.
- c) 64-bit key-space.

3. Let $M$ be a message that is signed using a secure signature algorithm $\text{sign}$ and a signature key $d$, producing a signature $C = \text{sign}(d, M)$. The corresponding public key is $e$.

- a) Does the signature $C$ have to be longer than $M$?
- b) Is the secret key $d$ required to verify that the signature is indeed valid? What about $M$?
- c) Can it be easy to convert the public key $e$ into the secret key $d$?
- d) Can it be easy to convert the secret key $d$ into the public key $e$?
- e) Can the message $M$ be derived from the signature $C$ using the public and/or secret key?

Try to think which options would violate the basic security requirements of a secure signature algorithm.