Timing Attacks:
determine a private key by keeping track of how long a computer takes to decipher messages.
Alarming for two reasons:

- It comes from a completely unexpected direction.
- It is a ciphertext-only attack.

Countermeasures:

- Constant exponentiation time.
- Random delay.
- Blinding.

Chosen Ciphertext Attack (CCA):
To counter such attacks, modifying the plaintext using a procedure known as optimal asymmetric encryption padding (OAEP).