Side Channel Attacks
- Timing
- Power
- Sound
- Light

- Usability and Security
  - Depending on Users
  - Role playing

- Modular Exponentiation

```
ModExp(m,e,n)  // M^e mod n
  Let e_l ... e_0 = e  // the bits of e
  Let acc = 1
  For i=0 … l
    if e_i = 1
      acc = acc*m mod n
      m = m^2 mod n
  return acc;
```

\[
m^e \mod n = m^{(2^0*e_0 + 2^1*e_1 + 2^2*e_2 + ... + 2^l*e_l)} \mod n
= m^{e_0} * (m^2)^{e_1} * (m^4)^{e_2} * (m^{(2^l)})^{e_l} \mod n
\]

- Power Analysis (smart cards)
- timing attack against square and multiply
  some reductions take longer than others
  - fast reductions
  - slow reductions
  - if attackers knows acc*m, he can predict whether reduction is fast or slow

attacker input \( m_0 \) \( m_1 \) \( m_2 \) \( m_3 \) \( \ldots \) \( m_k \)
time \( t_0 \) \( t_1 \) \( t_2 \) \( t_3 \) \( \ldots \) \( t_k \)

suppose \( e_0 = 1 \)
- can compute
  - acc and \( m \) at end of round 0
- predict whether end of round 1 will be fast or slow for each message \( m_i \)
- let
  - \( f \) = average time of "fast" messages
  - \( s \) = average time of "slow" messages

- two cases
  - \(| s_1 - f_1 | \) is small and \(| s_0 - f_0 | \) is small
    \( \Rightarrow e_1 = 0 \)
  - suppose \(| s_b - f_b | \) is large and \(| s(-b) - f(-b) | \) is small
    \( \Rightarrow e_1 = 1 \) and \( e_0 = b \)

repeat for round 2, \( \ldots \), \( l \)

- defense
  - for \( i=0 \) \( \ldots \) \( l \)
    - if \( e_i = 1 \)
      \[ \text{acc} = \text{acc} \times m \mod n \]
    - else
      \[ \text{tmp} = \text{acc} \times m \mod n \]
      \[ m = m^2 \mod n \]
- RSA binding
to compute $m^e \mod n$
  o pick random $r$
  o compute $x = (rm)^e \mod n$
  o compute $y = r^e \mod n$
  o return $x/y \mod n$