RSA Signature Scheme

- The original message is $M =$ "Security in Computing 2018"
- The hash of the message $h(M) = m = db1623867ac43b924848c0bc81a6e689$. If we do hex to decimal conversion $h(M) = m = 291215882146688649070551807467566065289$
- So, the message to be signed is
  $m = 291215882146688649070551807467566065289$
- Sender (Bob) Selects a random prime
  $p = 335011793073035265521070150212791157303$
- Sender (Bob) Selects a random prime
  $q = 185296104977565236504132463330798131651$
- Sender (Bob) Calculates
  $n = p * q$
  $= 335011793073035265521070150212791157303 * 185296104977565236504132463330798131651$
  $= 62076380377983504882775033807329459301827248264179403408279062206686444097253$
- Sender (Bob) Calculates
  $\phi(n) = (p-1) * (q-1)$
  $= 62076380377983504882775033807329459301306940366128802906253859593142854808300$
- Sender (Bob) chooses a prime number e, such that e is co-prime to $\phi(n)$, i.e, $\phi(n)$ is not divisible by e. Let's pick $e = 5737$
- Public Key is:
  $n = 62076380377983504882775033807329459301827248264179403408279062206686444097253, e = 5737$
- Private Key is:
  $d = 17312569043885934776440657851094149360657330414119938059962728838945192207 3$
- Bob signs the message (i.e. computes the signature) using private key as follows
  $s = m^d \ mod \ n$
  $= 291215882146688649070551807467566065289^{17312569043885934776440657851094149360657330414119938059962728838945192207 3} \ mod \ 62076380377983504882775033807329459301827248264179403408279062206686444097253$
  $= 27440668420937368156380618475781082504471439212562293630246944278146664956154$
- Bob sends the original message M and the signature of the message s
- Alice (receiver) verifies the signature using the public key of Bob
  $m' = s^e \ mod \ n$
  $= 27440668420937368156380618475781082504471439212562293630246944278146664956154^{5737} \ mod \ 62076380377983504882775033807329459301827248264179403408279062206686444097253$
  $= 291215882146688649070551807467566065289$ (in decimal)
  $= db1623867ac43b924848c0bc81a6e689$ (in hexadecimal)
  Alice also hashes the message $h(M) = m = db1623867ac43b924848c0bc81a6e689$ and finds that $h(M) = m = m'$. So, she accepts the message and the signature.