Week 3
Part 2 RSA continued...

RSA Digital Signature,

A Digital Signature is a digital world equivalent of physical handwritten signature. In physical world when we write a letter and put our signature, the first thing the signature proves is that the letter is indeed written by us. In the language of Cyber Security or Information Assurance, we this authenticity. The second important thing is, if i write a letter to any organization and put my signature on it and they wanna get back to me to ask more questions, i wont be able to deny that i was the one to write the ~~tot~~ letter at the first place because, whatever action i take in my official capacity, i have to be liable for that. Basically, any action we take, we cannot later deny it, if we take it in official capacity. In the language of Cyber Security, we call it nonrepudiation. Digital Signature perform two important operations, Authenticity and Nonrepudiation, when we talk about only digital signature, Confidentiality is not a major goal. Confidentiality means secrecy of information.

Previously we learned that RSA is symmetrical. Means when we encrypt something with RSA, we use the Public key and when we decrypt, we use the Private key. For encryption we use the public key first then use the Private key later, We can change the order of the operation, we can start with the Private key and finish it with the public key. This happens when we perform Digital Signature with RSA.

RSA Digital Signature,

The initial part of the math is same as we followed before for RSA encryption.

$P = 3$ and $q = 11$

$Pq = 3 \times 11 = 33$

$(P-1) \times (q-1) = 2 \times 10 = 20$

we need to choose an e that is relatively prime to 20,

Let's say $e = 7$

Compute a value of d such that $(d * e) \% 20 = 1$

$d = 3$

Public key is $(e, 33) = (7, 33)$

Private key is $(d, 33) = (3, 33)$

Let's assume our message is $m = 4$

Now, for digital signature we will be using the private key first.

Generate Signature: → Private key

The signature = $m^d \bmod (Pq)$

$= 4^3 \bmod 33$

$= 31$

The sender will send (4, 31) to the receiver

The receiver recieves (4, 31)

Verify signature,

$= 31^{e} \bmod 33$

$= 31^{7} \bmod 33$

$= 4$

Signature verified