Schnorr Digital Signature

- Also uses exponentiation in a finite (Galois)
- Minimizes message dependent computation
  - Main work can be done in idle time
- Using a prime modulus p
  - $p-1$ has a prime factor q of appropriate size
  - typically p 1024-bit and q 160-bit (SHA-1 hash size)
- Schnorr Key Setup: Choose suitable primes p , q
  - Choose a such that $a^q = 1 \bmod p$
  - (a,p,q) are global parameters for all
  - Each user (e.g., A) generates a key
  - Chooses a secret key (number): $0 < s < q$
  - Computes his **public key**: $v = a^{-s} \bmod q$

- User signs message by
  - Choosing random r with $0<r<q$ and computing $x = a^r \bmod p$
  - Concatenating message with x and hashing:

$$e = H(M \,||\, x)$$

  - Computing: $y = (r + se) \bmod q$
  - Signature is pair (e, y)
- Any other user can verify the signature as follows:
  - Computing: $x' = a^y v^e \bmod p$
  - Verifying that: $e = H(M \,||\, x')$
  - $x' = a^y v^e = a^y a^{-se} = a^{y-se} = a^r = x \bmod p$

- Signature is valid only if $x' = x$.