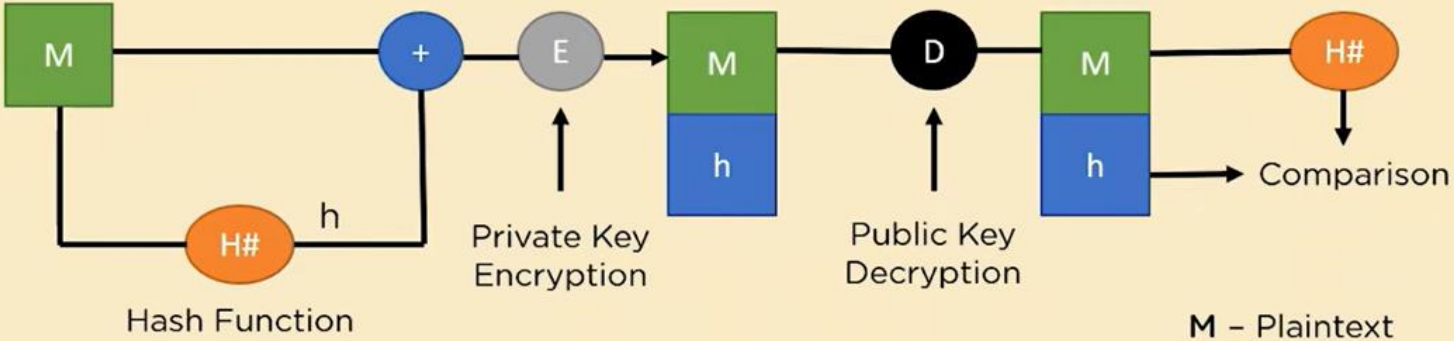
CYBER ENRICH TRAINING PROGRAM | MODULE III

Digital Signature

What Are Digital Signatures?

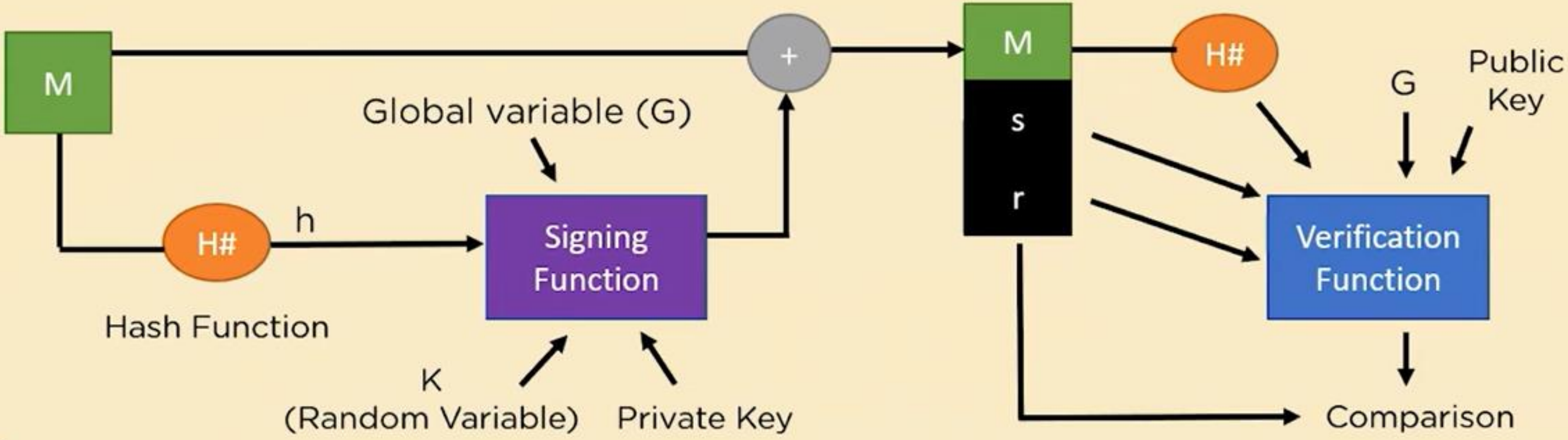
- Mechanism to **determine authenticity** of a document file
- Uses **public key** cryptography mechanism
- Helpful to authenticate **long distance** official communication channels



M – Plaintext
h - Digest

What Is DSA?

- Federal Information Processing Standard for **digital signatures**.
- Proposed in 1991, standardized in **1994**.
- National Institute of Standards & Technology made it **royalty free**.
- Covers the process from key **generation** to signature **verification**.



Step 1: Key Generation

1. Pre-requisites for the key generation formulas:

   - **q** -> Prime Divisor

   - **p** -> prime number, such that : p-1 mod q = 0

   - **g** -> any integer (1<g<p) such that : g**q mod p = 1 and g = h**((p–1)/q) mod p

Step 1: Key Generation

- **x (private key)** -> random integer such that : $0 < x < q$
- **y (public key)** can be calculated as : $y = g^x \bmod p$
- Private Key can be packaged as : $\{p,q,g,x\}$
- Public Key can be packaged as : $\{p,q,g,y\}$

Step 2: Signature Generation

1. Message is passed through a hash function to generate a **digest (h)**.

2. Choose any random integer **k** such that : $0 < k < q$

3. To calculate the value of **r** :

   $(g^{k} \text{ mod } p) \text{ mod } q$

4. To calculate the value of s :

   $[K^{-1}(h+x \text{ . } R)\text{mod } q]$

The Signature can be packaged as $\{r,s\}$

Step 3: Signature Verification

1. Calculate the message digest using **same hash function**.

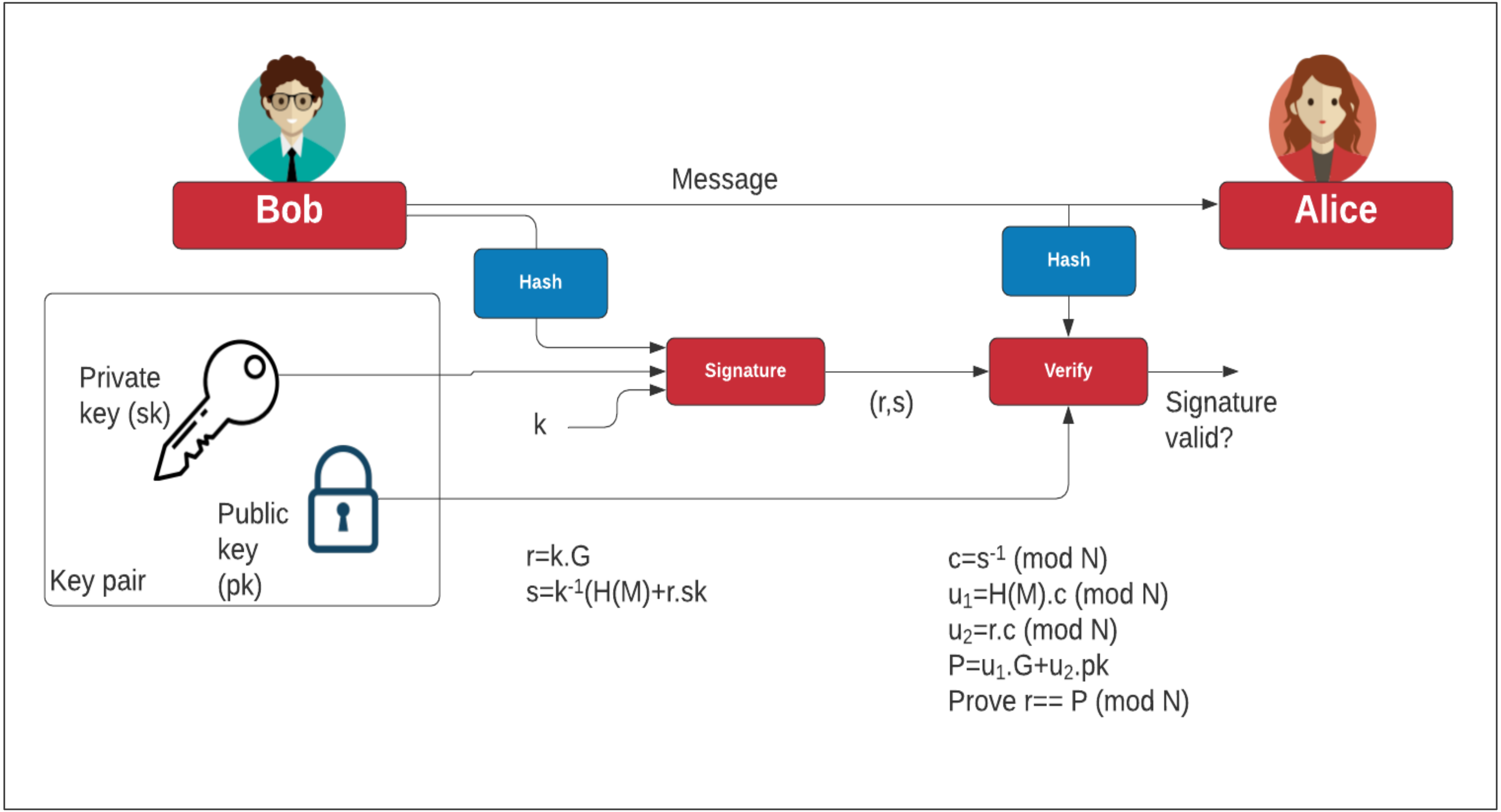
2. Compute the value of **w** such that :
   $s*w \bmod q = 1$

3. Compute the value of **u1** as :
   $u1 = h*w \bmod q$

4. Compute the value of **u2** as :
   $u2 = r*W \bmod q$

5. Finally, the verification component v :
   $v = [((g^{u1} . y^{u2}) \bmod p) \bmod q]$

If v ==r, the signature verification is succesfull.



$r=k.G$

$s=k^{-1}(H(M)+r.sk$

$c=s^{-1}$ (mod N)

$u_1=H(M).c$ (mod N)

$u_2=r.c$ (mod N)

$P=u_1.G+u_2.pk$

Prove r== P (mod N)