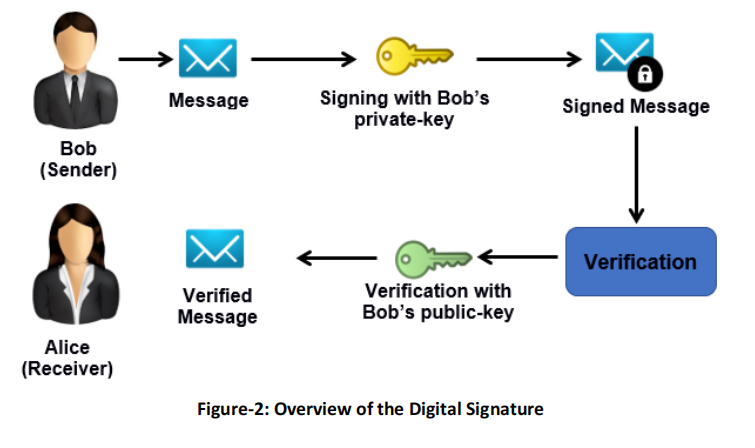
**Digital Signature Algorithm (DSA)**

* A digital signature ensures the authenticity and integrity of digital messages or documents.
* DSA is a method proposed by NIST in 1991 to create secure digital signatures.
* DSA secures communications by verifying the authenticity and integrity of data.

## **What is Digital Signature?**

A digital signature verifies authenticity but doesn’t ensure confidentiality. To keep the message private, you need to encrypt both the message and the signature using a secret key or public key system. This adds an extra layer of security to the digital signature process.

Example:

* Alice encrypts a message using Bob's public key, ensuring only Bob can decrypt it with his private key.
* Bob wants to confirm the message actually came from Alice and not from an imposter like Eve.
* Alice adds her digital signature to the message, proving her identity and ensuring the message's authenticity.

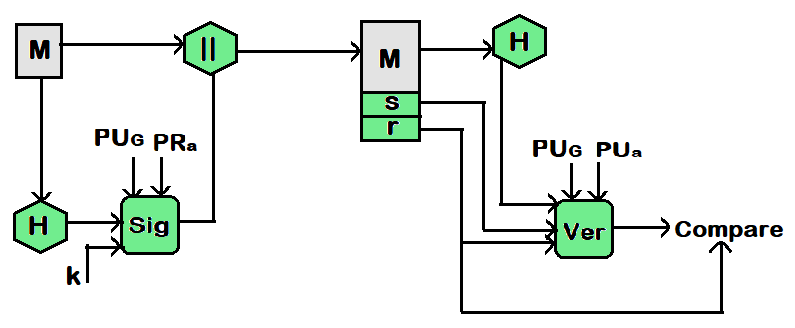
## Method of Digital Signature

These two are standard Approaches to implement the Digital Signature:

* Rivest-Shamir-Adleman (RSA)
* Digital Signature Algorithm (DSA)

## Digital Signature Algorithm (DSA)

* DSA generates a hash code combined with a random number and the sender's private key to create a signature.
* A shared global public key (PUG) is used by all communicating parties for signature generation and verification.
* The digital signature consists of two parts, s and r, generated by the signature function.
* The receiver generates a hash code and verifies the signature using the sender’s public key and global public key.
* If the verification function outputs rrr, the signature is valid and confirms the sender’s authenticity.



* M = Message or Plaintext
* H = Hash Function
* || = Group the plantext and hash function (hash digest)
* E = Encryption Algorithm
* D = Decryption Algorithm
* PUa = Public key of sender
* PRa = Private key of sender
* Sig = Signature function
* Ver = Verification function
* PUG = Global public Key

## Steps to Perform DSA

1. **Global Public-Key Components :**

 **Prime Number p**: A prime number p is chosen with a bit length between 512 and 1024 (in increments of 64), such that q divides (p−1)(p - 1)(p−1).

 **Prime Number q**: A smaller prime number q, the divisor of (p−1)(p - 1)(p−1), is selected with a bit length N, satisfying 2N−1<q<2

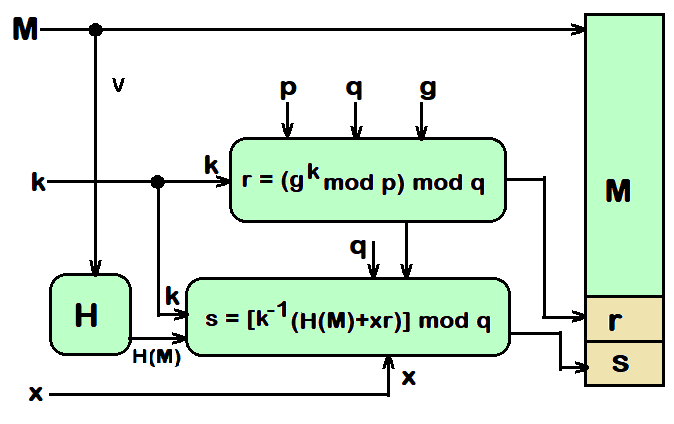
1. **User Private Key:**

The private key x is a number that is chosen randomly or pseudorandomly. It must be between 1 and q−1 meaning x is a random integer within this range (0 < x < q).

1. **User Public Key:**

The public key y is calculated as y=g^x mod  p and while it's easy to compute y from x, it's very difficult to find x given y, which is known as the discrete logarithm problem.

1. **Signing:**

 To create a signature, the user calculates two values, r and s, using the public key components (p, q, g), the message hash H(M), the private key x, and a randomly generated integer k (where 0<k<q) that is unique for each signature.

1. **Verification:**

The receiver calculates a value v using the public key components, the sender's public key, and the message hash. If v matches the r value from the signature, the signature is considered valid.

## Services Provided By DSA

 **Message Authentication**:  
A digital signature ensures that the message was sent by the claimed sender (e.g., Alice), as only her public key can verify her signature. It prevents Eve from impersonating Alice.

 **Message Integrity**:  
A digital signature ensures message integrity by using a hash function, so any change in the message would result in a different signature during verification.

 **Nonrepudiation**:  
Nonrepudiation ensures Alice cannot deny sending a message by keeping a signed message with a timestamp from a trusted third party. This trusted center can authenticate and provide evidence if Alice denies sending the message.

## Advantages of DSA

 **Authentication**: Digital signatures provide strong identity authentication, ensuring the sender is verified.

 **Integrity**: Digital signatures ensure that the content remains unchanged; any alteration makes the signature invalid.

 **Non-Repudiation**: Digital signatures prevent the sender from denying their involvement in creating the document.

 **Efficiency**: Digital signatures automate signing, enabling fast and secure online transactions without manual verification.

 **Security**: Digital signatures, backed by public key cryptography and hashing, ensure protection against forgery.

## Disadvantages of DSA

 **Key Management Complexity**: Properly generating, storing, distributing, and revoking cryptographic keys is a complex but necessary process for digital signatures.

 **Infrastructure Dependence**: Digital signatures rely on secure Public Key Infrastructure (PKI), and any compromise can affect their trustworthiness.

 **Legal and Regulatory Challenges**: Digital signatures may face legal and regulatory challenges depending on local laws and standards.

 **Initial Setup Costs**: Setting up a digital signature system involves costs for certificates, security measures, and user training.

 **Offline Usability**: Digital signatures may be problematic without access to the signer's private key, and hardware tokens add complexity.