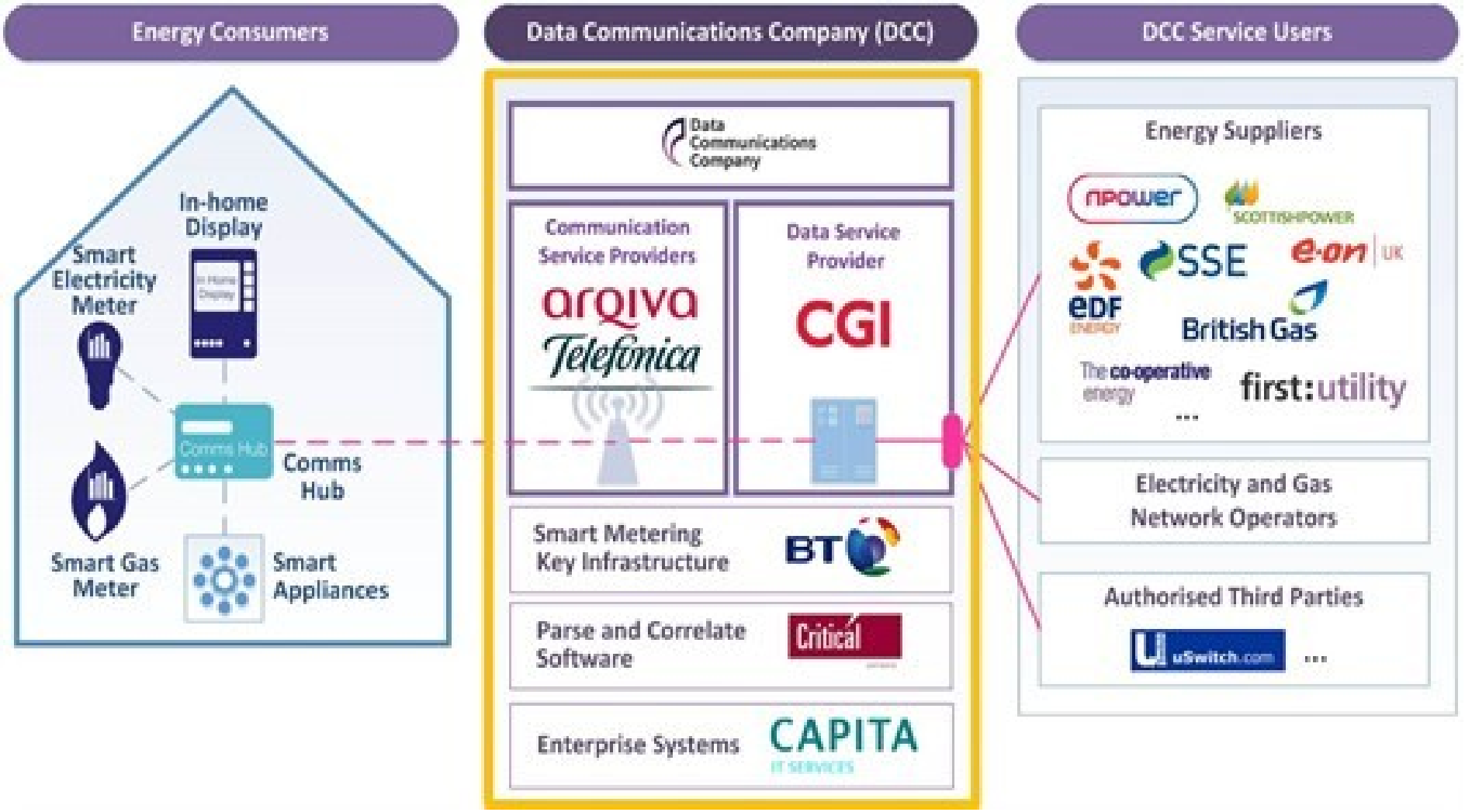
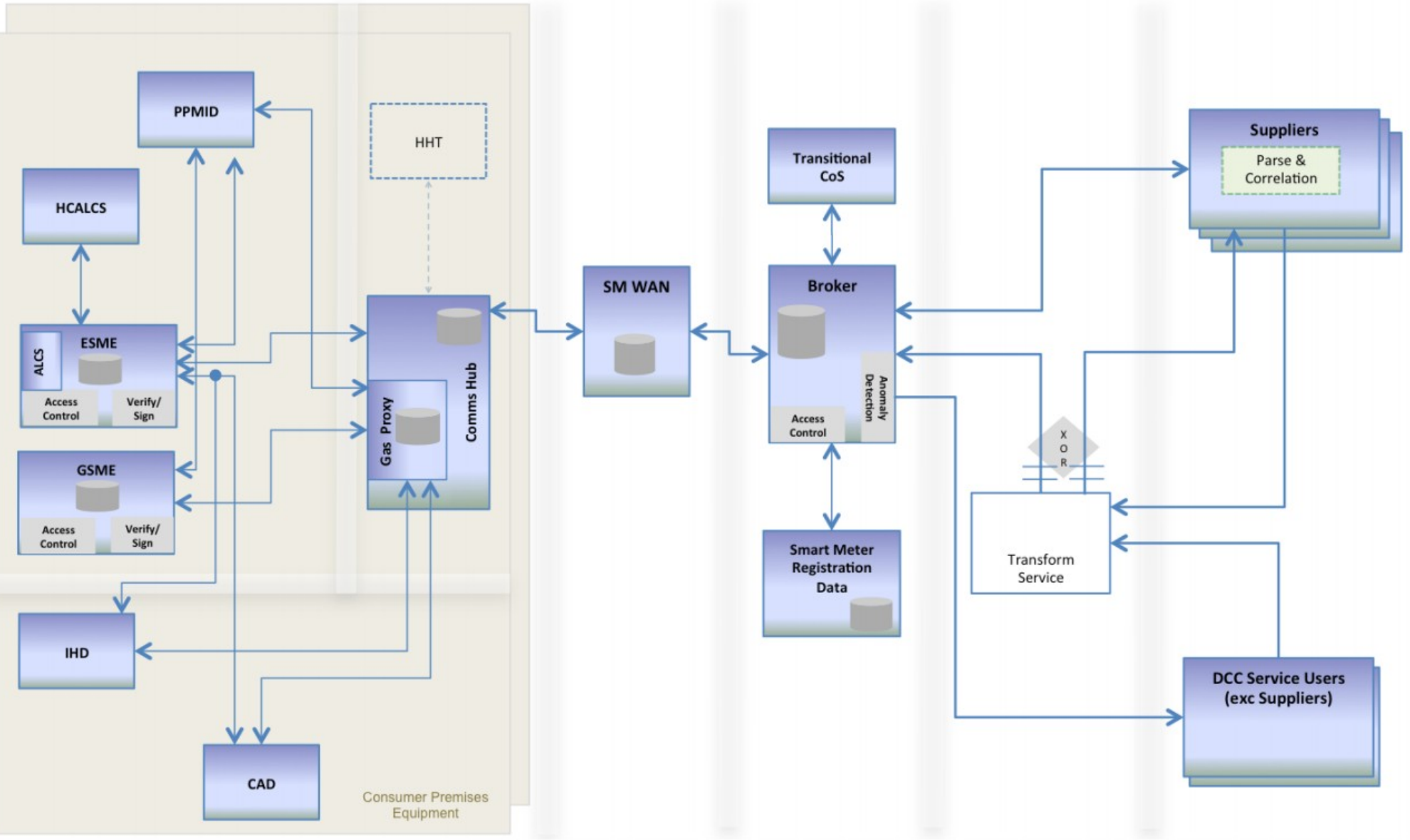
# Smart Metering Concept




Ref.: https://www.smartdcc.co.uk/about-dcc/




Ref.:
https://www.google.co.in/url?sa=t&rct=j&q=&esrc=s&source=web&cd=7&ved=0CD4QFjAGahUKEwjXvo322KLHAhUCxI4KHWq9AL4&url=https%3A%2F%2Fwww.cesg.gov.uk%2Fpublications%2FDocuments%2FSmartMeteringHANConnectedALCS.PDF&ei=3snKVdfXDoKIuwTq-oLwCw&usg=AFQjCNE3cZU3ek5L-n-x5utwfwDBAkLf6A&bvm=bv.99804247,d.c2E&cad=rja

# What is Cryptography?

- Origin from Greek word “Kryptos” meaning “Secret Writing”
- Provides Various aspects of information security such as,

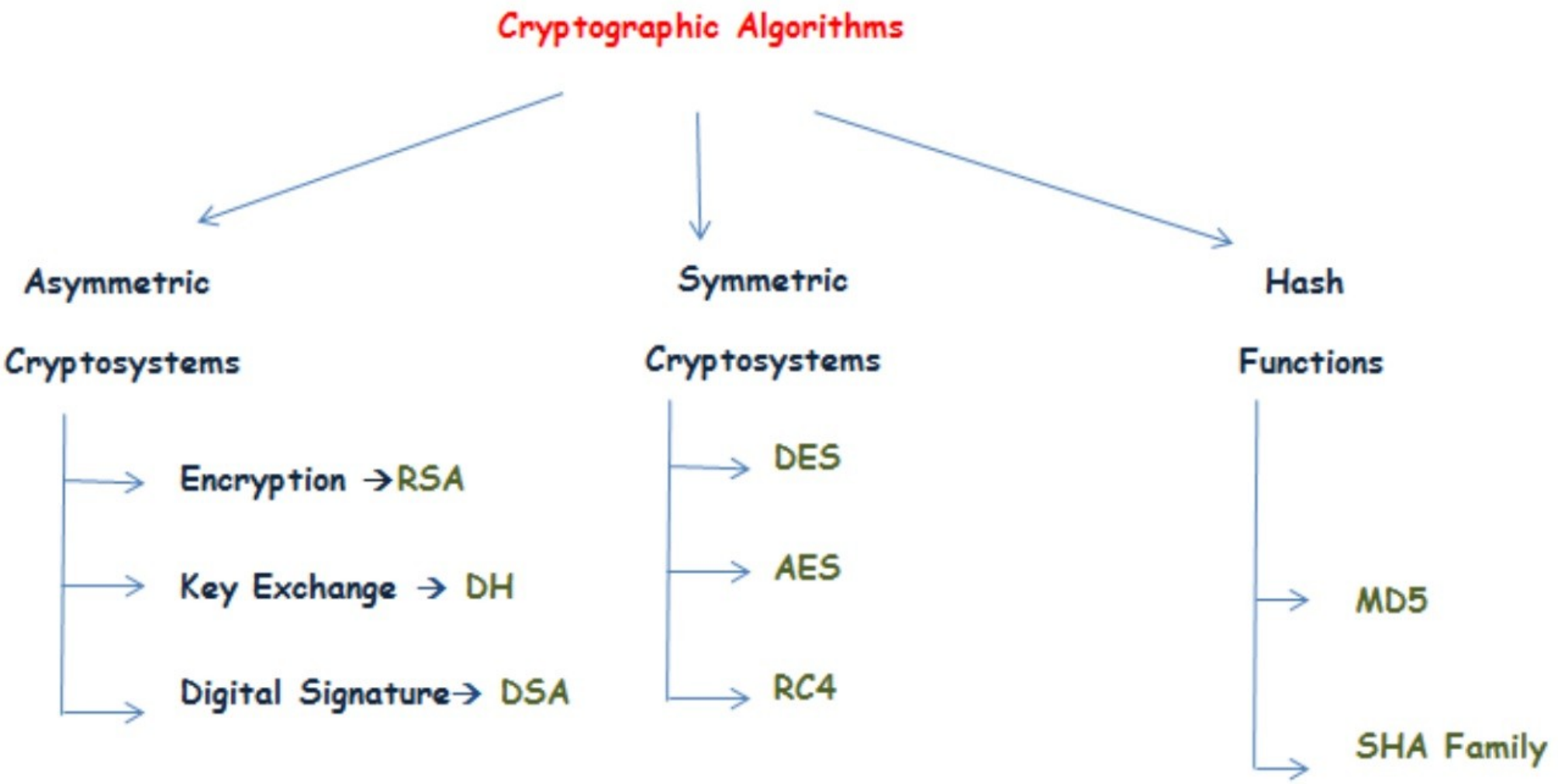
  ->Data Confidentiality,

  ->Data Integrity,

  ->Authentication,

  -> Non-Repudiation

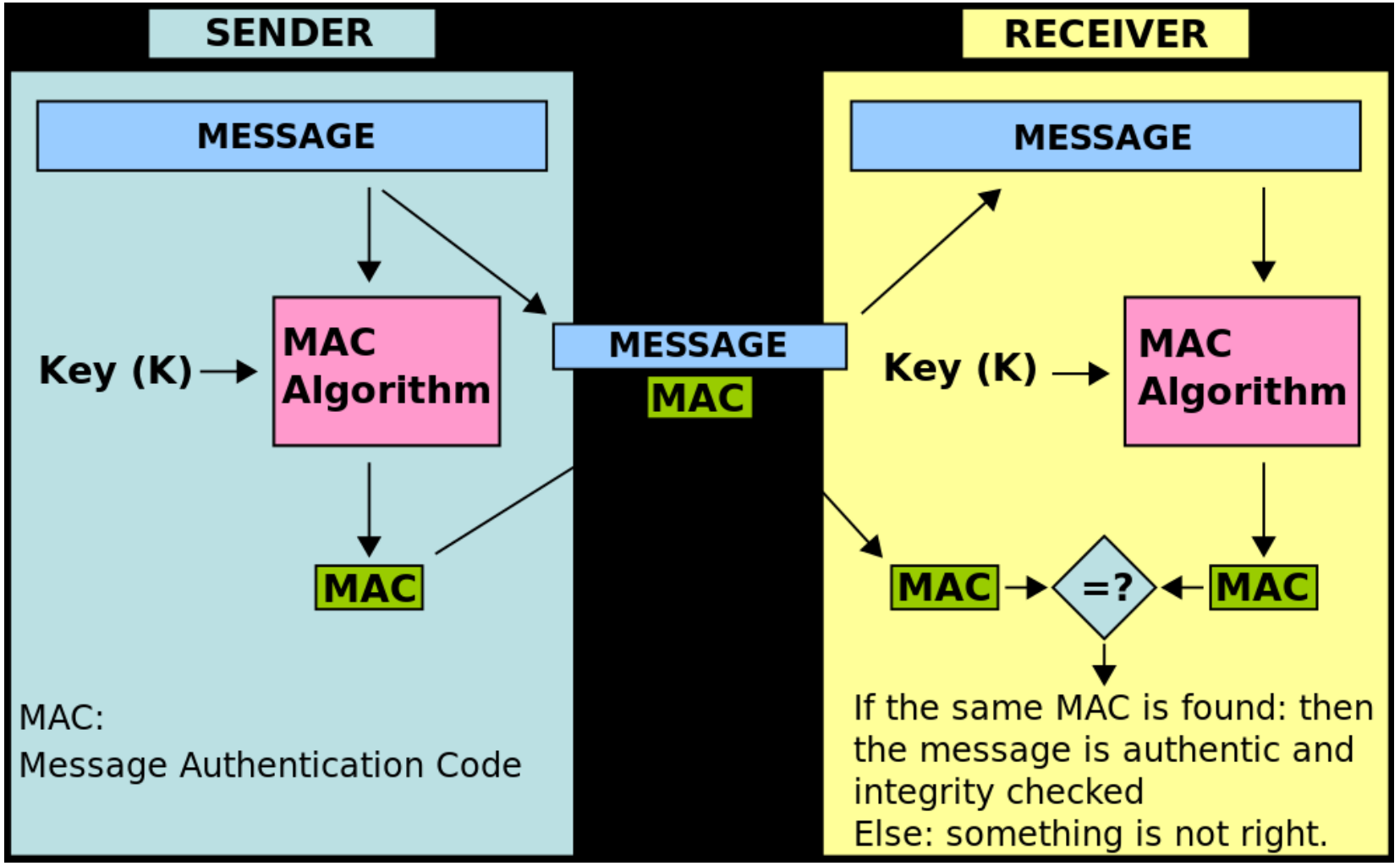
# Cryptographic Algorithm classification



# Public Key Cryptography

- One-way function
- Relatively easy to compute f(x) but extremely difficult to compute x, given f(x)
- Not used for encryption
- Used in One way Hash function-> Message Digest,finger prints,integrity checksum
- Function takes variable length input(message), computes a smaller fixed length output called Hash value of Message Digest: M->Hash Function->H(M)
- No secrecy is needed as hash is a public function
- Variant of one-way Hash is Encrypted Hash, known as **Message Authentication Code(MAC)**
- MAC is a function of shared secret key, so that possessor of the key can verify the integrity of the message
- This implies that the sender and receiver of a message must agree on the same key before initiating communications, as is the case with symmetric encryption, this procedure is called key agreement
- In contrast to digital signature, MAC does not provide Non-Repudiation

# MAC Construction & Confirmation




Key(K) is computed both side by using Public-Private Key pair **(Diffie-Hellman exponential key exchange)**

# ISO Authentication Framework

- ISO introduced a set of protocols known as **X.509** protocols to provide standards for authentication across networks
- The most important part of the ISO framework is the structure for public key certificates
- Each user has a unique name (called a distinguished name) that is a collection of several attributes including the user's real name, organization, locality, and country
- A trusted Certification Authority (CA) issues a signed certificate that **contains** the distinguished name and the user's public key
- The certificate is signed by the CA
- The certificate looks like this,

| version | serial # | algorithm, params | issuer | validity: from, to | distinguished name | Pub. Key: alg, params, key | signature of CA |
|---|---|---|---|---|---|---|---|

# Cont.

- If A wants to talk to B and they have a common CA, A can get B's certificate from some database (or some source). A can then verify the signature of the CA (by hashing the contents of the certificate and comparing them with the CA's signature decrypted with the CA's public key). This gives A assurance that B's certificate was indeed generated by the same certification authority.

- What is Certificate Chaining?

  Certification authorities are designed to fit into a hierarchical structure. Each CA has a certificate signed by the CA above it and by the CA below it. If you have a certificate signed by an unknown CA, you can ask the CA for its key and see which higher-level signed it. If that is also unknown, you can repeat the process until a CA is reached (a common root). This is known as **certificate chaining**.

# Cont.

- Certificate Path Validation (CPV)

-> Before a certificate can be used, it must be validated.

CPV is the algorithm which verifies that a given certificate path is valid under a given public key infrastructure (PKI). A path starts with the Subject certificate and proceeds through a number of intermediate certificates up to a trusted root certificate, typically issued by a trusted Certification Authority (CA).

Public Key Infrastructure (PKI) supports a number of security-related services, including data confidentiality, data integrity, and end-entity authentication. Fundamentally, these services are based on the proper use of public/private key pairs. The public component of this key pair is issued in the form of a public key certificate and, in association with the appropriate algorithm(s), it may be used to verify a digital signature, encrypt data, or both.

-> Certificate Path Processing?

A process in which a chain of certificates or a certification path between the certificate and an established point of trust must be established, and every certificate within that path must be checked.

# Cont.

In general, certification path processing consists of two phases,

1) Path construction

-> building one or more candidate certification path

2) Path validation

-> making sure that each certificate in the path is within its established validity period, has not been revoked

- **Certification Revocation List(CRL)**

  ->CA is responsible for maintaining a Certificate Revocation List(CRL)

  ->Certificate has Validity period defined by CA

  -> Anytime certificate is presented as part of authentication dialog, a current time should be check against its validity period

  -> if certificate is past that period,or expired,then authentication should failed.

# Cont.

- However, sometimes Certificate should not honored even during its validity period.
- For example, if the private key associated with a certificate is lost or exposed, then any authentication using that certificate should be denied and has to be replaced by new one.
- When their certificates are replaced, the old certificates have to be marked somehow as “no longer accepted”.
- The purpose of the CRL is to list certificates which are valid, but are revoked.
- CRL is generated and published periodically , often at defined interval.
- CRL is always issued by the CA which issues the corresponding certificate.
- All CRL have a lifetime during which they are valid; this lifetime is often 24hours or less

# Galois Counter Mode(GCM)

- Used for Authenticated Encryption with associated data
- Constructed from symmetric key block cipher with block size of 128 bit.
- GCM is a mode of operation of the AES algorithm.
- Assurance of authenticity is provided from Hash function that is defined over a binary Galois.
- If GCM input is restricted to data that is not to be encrypted, the resulting specialization of GCM, called GMAC.
- GMAC,

  -> Galois MAC, is a authentication-only variant of the GCM which can be used as an incremental message authentication code.

  ->Both GCM and GMAC can accept initialization vectors of arbitrary length.

# Elliptic Curve Digital Signature Algorithm

- It is a Elliptic Curve analogue of DSA.
- First proposed in 1992 by Scott Vanstone in response to NIST's RFC
- Accepted in 1998 as an ISO 14888-3 , in 1999 as an ANSI X9.62 and in 2000 as an IEEE 1363-2000 & FIPS 186-2.
- ECDSA concerned with “Asymmetric” means that each entity select key pair consisting of related private key and public key.
- The entity maintains the secrecy of the private key which it uses for signing messages, and makes authentic copies of its public key available to other entities which use it to verify signatures.