Lesson 7
Access Control and Secure Message Communication

Standard Authorisation Models

- Access Control List (ACL) for coarse grain access control
- Role-based Access Control (RBAC) for fine grain access control
- Attribute-based Access Control (ABAC) or other capability-based fine grain access control

Central access control server

- Data communication gateway can be centrally used to controlled accesses between application/service and IoT devices.
- The server central control, on a cloud server
- Each device can access the server and communicate data to other server

A Distributed Architecture

Enables:

1. Each device to request the access to server and the server grants application/service access token for the or
2. Each application/service to request the access to server and the server grants device access token for the device.

Key Generation, Exchange and Management

- Key generation and exchange for the authentication and authorisations followed by secure communication of an application/service message to the device/ gateway.

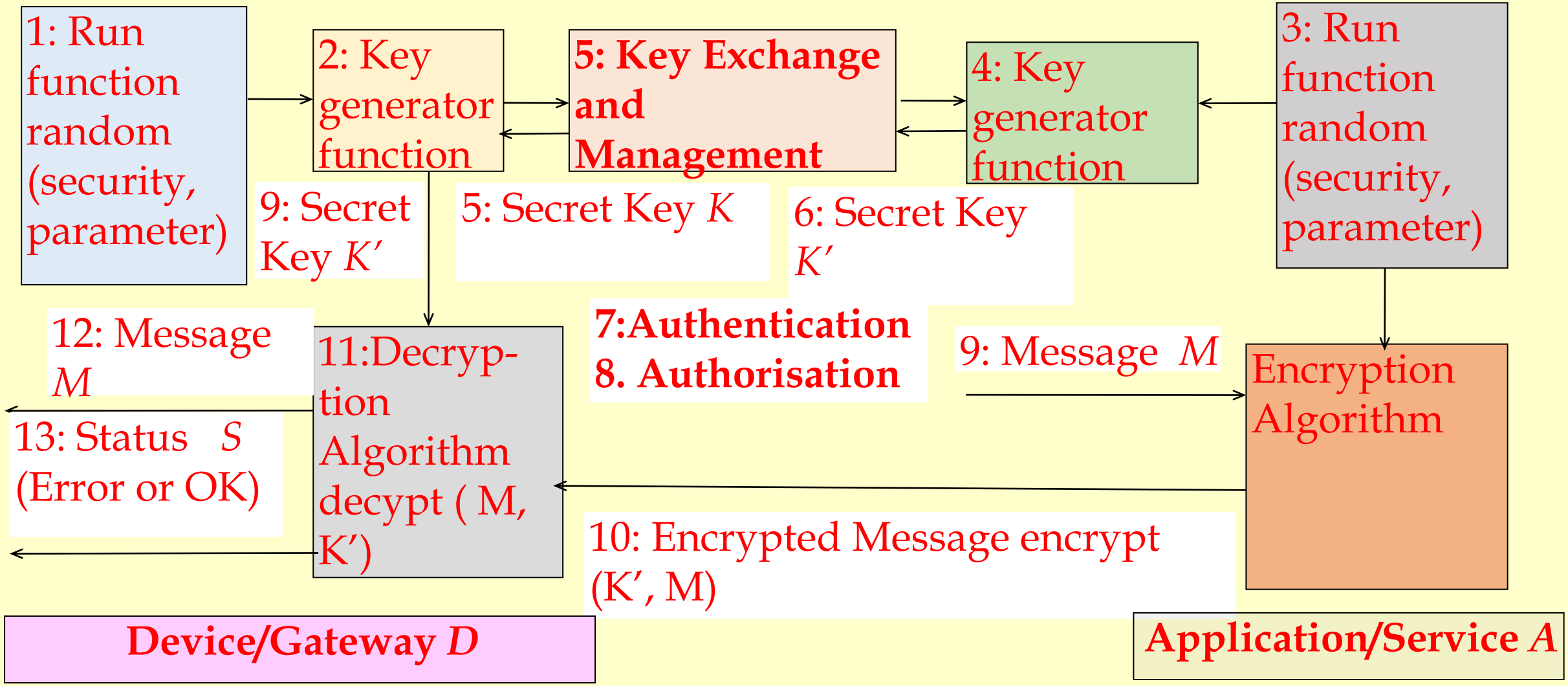

Fig. 10.5 Steps during Key exchanges and management, Authentication and authorizations followed by secure communication of Application/Service Message to the Device/Gateway

Message-Integrity Check Steps

1. Retrieve *M any time later. Assume that retrieved message is M1.*
2. Calculate 128 or 192 or 256 Hash value *h1, taking the message M1 and K as inputs.*
3. Compare *h1 and h0.*
4. Message is unchanged if *h1 = h0, and integrity check passes else fails.*

- Message or data integrity means maintaining and assuring the accuracy and consistency over its entire life-cycle.

Message Non-Repudiation

- Means an assurance that source of message once communicates data to a sender, later on cannot deny that the message is not from the source and not same as sent earlier.
- Means data is signed and signature put at the source cannot be said to be not that of the source and the message is thus not from that source
- Digital signature method which ensures non-repudiation

- A service provides the proof of message origin as well as message integrity. A digital
- certificate asserts the origin using a public key infrastructure. A digital signature is
- certified by trusted digital certifying service [trusted third party (TTP) service]. TTP
- protects the private (secret) key and issues the certificate that message was sent using this
- specific private (secret) key of source if private key is lost and used by some other source
- of message. Only the TTP is permitted to be the repository for public key certificates.

Digital Certificate from trusted third party (TTP) service

- Digital certificate asserts the origin using a public key infrastructure
- TTP certifies digital signature
- TTP protects the private (secret) key and issues the certificate that message was sent using this specific private (secret) key of source if private key is lost and used by some other source of message
- Only the TTP permitted to be the repository for public key certificates.

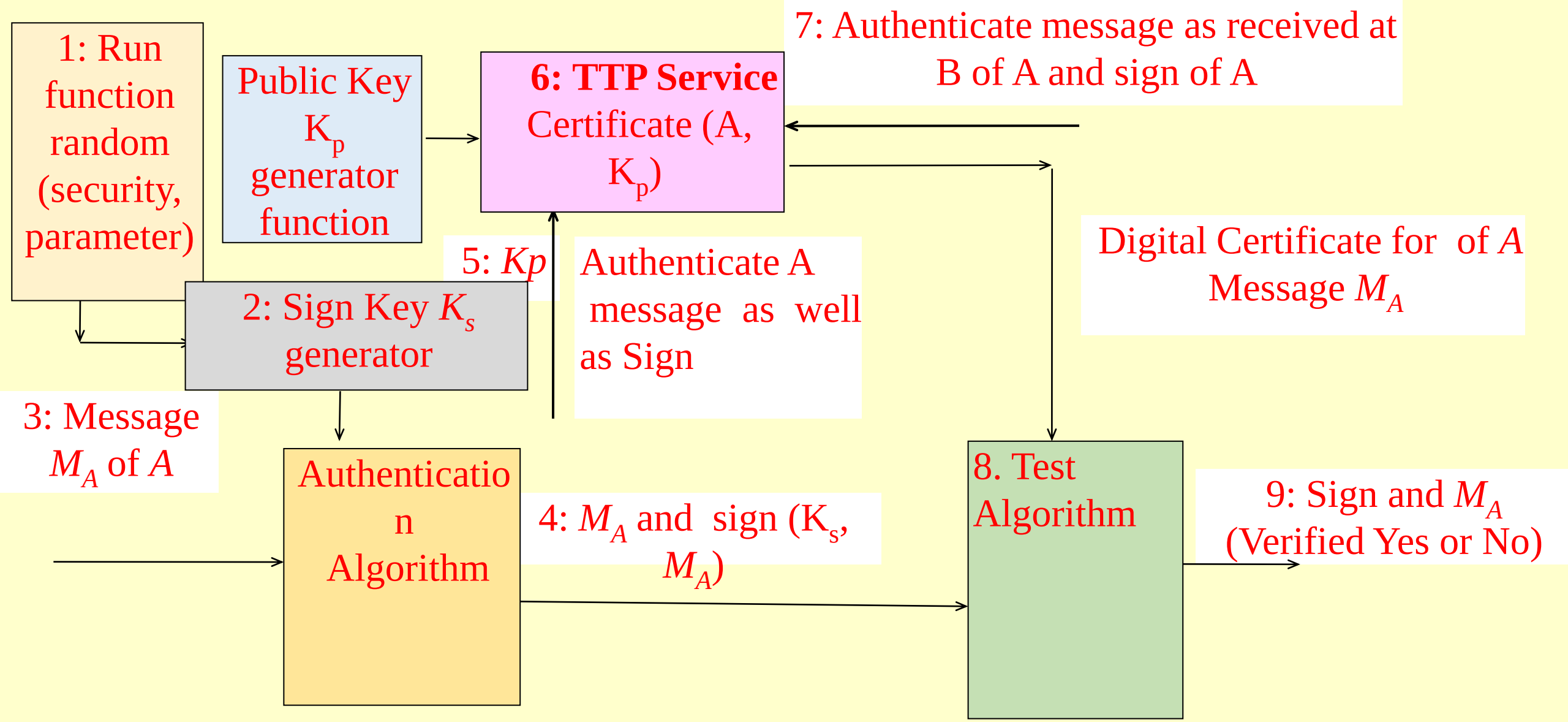

Fig. 10.6 Use of TTP Service and steps for signing, issue of digital certificates to a signed message and verification of signed message

Message unavailability due to Denial of Service Attack

- ICMP flooding which repeatedly send the control messages to destination and thus deny the path to source end
- An SYN flood which means attacker sends flood of TCP/SYN messages (packets) using a forged address, and destination sends repeatedly TCP/SYN packets assuming the packet from actual source.

Attacks On Message Availability

- The service to the source message becomes unavailable.
- At the Destination original message becomes unavailable
- Peer-peer attack
- Application layer messages flooding

Solution of Attacks on Message Availability

- Prevented using specific methods for specific type of attacks
- Firewall, a method for preventing the attacks the message from un-trusted networks

Summary

We learnt

- Essential elements of access control: Id establishment and authentication
- The sender stands authenticated using hash values
- A hash function or MD5 gives the irreversible result after many operations on that and the operations are just one way

Summary

We learnt

- Message-integrity must need to be checked using hash
- Key need to be exchanged before the authentication code, authorisation commands and encrypted messages communicate.
- Message availability affected due to DoS Attacks
- Non-repudiation
- Digital sign functions

Summary

We learnt

- A TTP service issues digital certificate for the message and sign, and saves in repository
- Message availability ensured by prevention of ‘Denial of Service’ attacks

End of Lesson 7 on Access Control and Secure Message Communication