
# CCNA Security – Part III

## Virtual Private Networks (VPN)

**Based on CCNA Security 210-260 Official Cert Guide**

# Chapter 5

Fundamentals of VPN Technology and Cryptography

# Fundamentals of VPN Technology

Teknologisk videncenter – en del af mercantec

- Understanding VPNs and why we use them
- Cryptography basic components
- Public key infrastructure
- Putting the pieces of PKI to work

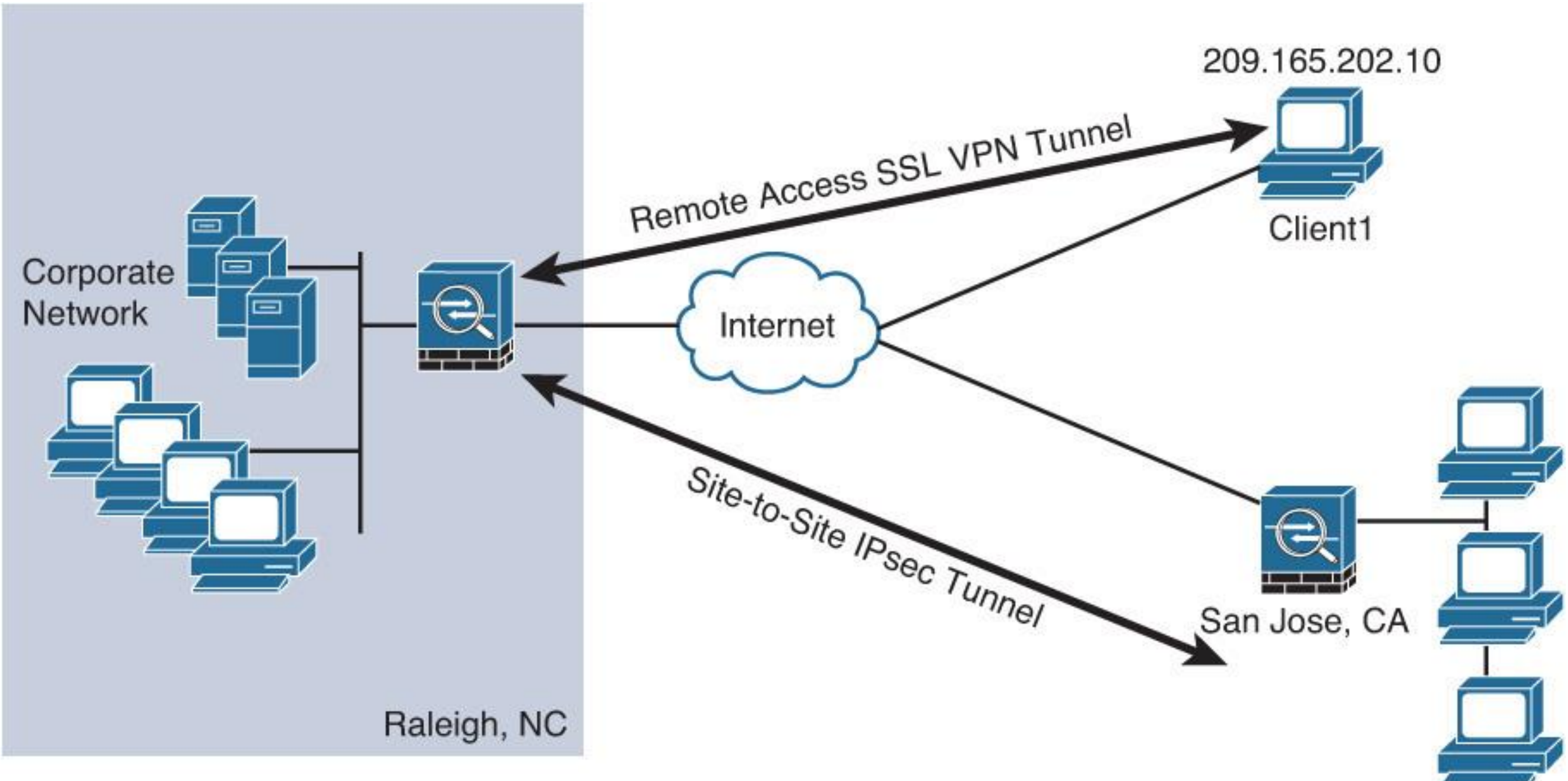
# Types of VPN technologies

Teknologisk videncenter – en del af mercantec

- IPsec
  - Implements security of IP packets at Layer 3 of the OSI model, and can be used for site-to-site VPNs and remote-access VPNs.
- SSL
  - Secure Sockets Layer implements security of TCP sessions over encrypted SSL tunnels of the OSI model, and can be used for remote-access VPNs (as well as being used to securely visit a web server that supports it via HTTPS).
- MPLS
  - Multiprotocol Label Switching and MPLS Layer 3 VPNs are provided by a service provider

# Two main types of VPN's

- Remote-Access VPN
- Site-to-Site VPN



# Main benefits of VPN’s



- Confidentiality
  - Confidentiality means that only the intended parties can understand the data that is sent.
- Data integrity
  - Data can not be changed or modified in transit – receiver will notice
- Authentication
  - Identity of remote user known
- Antireplay protection
  - Packet or packet sequence cannot be retransmitted

# Ciphers and keys

- A cipher is a set of rules or algorithms how to perform encryption and decryption
  - **Substitution:** This type of cipher substitutes one character for another (CAESAR)
  - **Polyalphabetic:** This is similar to substitution, but instead of using a single alphabet, it could use multiple alphabets and switch between them by some trigger character in the encoded message (ENIGMA)
  - **Transposition:** This uses many different options, including the rearrangement of letters. Modern Ciphers use complex forms of transpositions called block ciphers.

# Block and stream ciphers

Teknologisk videncenter – en del af mercantec

- Block Ciphers
  - A block cipher is a symmetric key (same key to encrypt and decrypt) cipher that operates on a group of bits called a block. A block cipher encryption algorithm may take a 64-bit block of plain text and generate a 64-bit block of cipher text.
  - Advanced Encryption Standard (AES)
  - Triple Digital Encryption Standard (3DES)
  - Blowfish
  - Digital Encryption Standard (DES)
  - International Data Encryption Algorithm (IDEA)

# Stream ciphers

- Stream Ciphers
  - A stream cipher is a symmetric key cipher (same key to encrypt as decrypt), where each bit of plaintext data to be encrypted is done 1 bit at a time against the bits of the key stream, also called a cipher digit stream
  - An advantage of stream ciphers in military cryptography is that the cipher stream can be generated in a separate box that is subject to strict security measures

# Symmetric encryption Algorithms

Teknologisk videncenter – en del af mercantec

- Symmetric algorithm
  - Use the same key to encrypt and decrypt
  - Key distribution: How will the intended receiver get the key
- Examples:
  - DES - Data Encryption Standard
  - 3DES – Triple DES
  - AES – Advanced Encryption Standard (Best practice)
  - IDEA - International Data Encryption Algorithm
  - RC2, RC4, RC5, RC6 - Rivest cipher
  - Blowfish

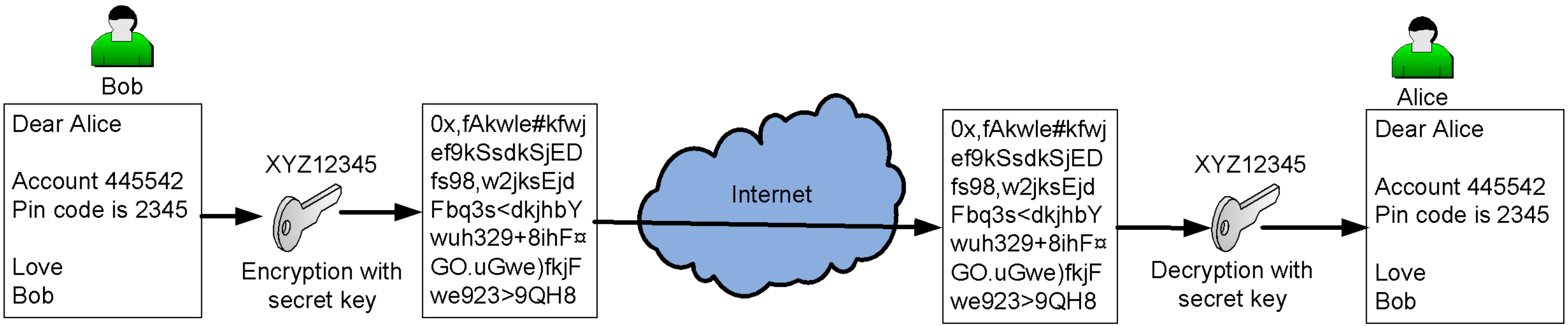
# Asymmetric Algorithms

Teknologisk videncenter – en del af mercantec

- Asymmetric algorithms use different encryption and decryptions keys
- The keys are mathematically bound together
- High cost in CPU power
- Examples:
  - RSA - Named after Rivest, Shamir, and Adleman, who created the algorithm
  - DH - Diffie-Hellman key exchange protocol

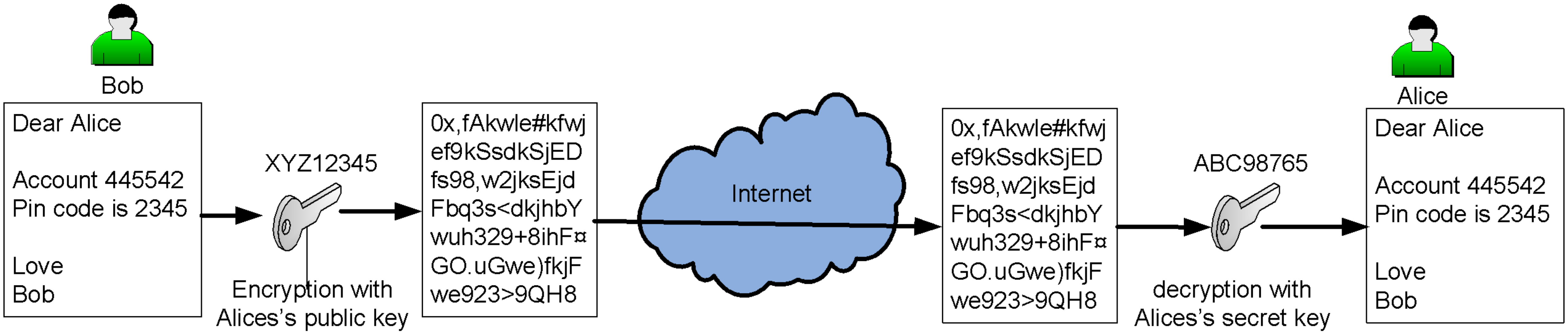
# Encryption: Symmetrical keys

- Same key used with encryption and decryption
- Symmetrical cipher examples:
  - DES: 56 bit key
  - 3DES: three different 56 bit keys
  - AES: 128, 192 and 256 bit keys



# Encryption with  Asymmetric keys

- Assymetrical keys uses different keys for encryption and decryption
- Alice generates a public and a secret key. The public key is sent to Bob
- Bob encrypts his message with the public key and transmits the encypted message to Alice
- Alice decrypts the message with the secret key.
- RSA is a assymmetric encryption cipher
  - Key size 1024 to 4096 typical



# Diffie and Hellman



- Dr. Whitfield Diffie
- Bachelor of science mathmatics
- Retired but studying security in grid computing

- Martin Hellman
- Professor Emeritus from Stanford University
- Retired

# Diffie-Hellman key exchange

- Uses mathematical one-way functions
- Security based on huge prime numbers
  - Brute force attacks would take years
- Mathematics out of scope in this course
- Different Diffie-Hellman groups
  - DH Group 1 = 768 bit
  - DH Group 2 = 1024 bit
  - DH Group 5 = 1536 bit
- Higher group numbers are more secure

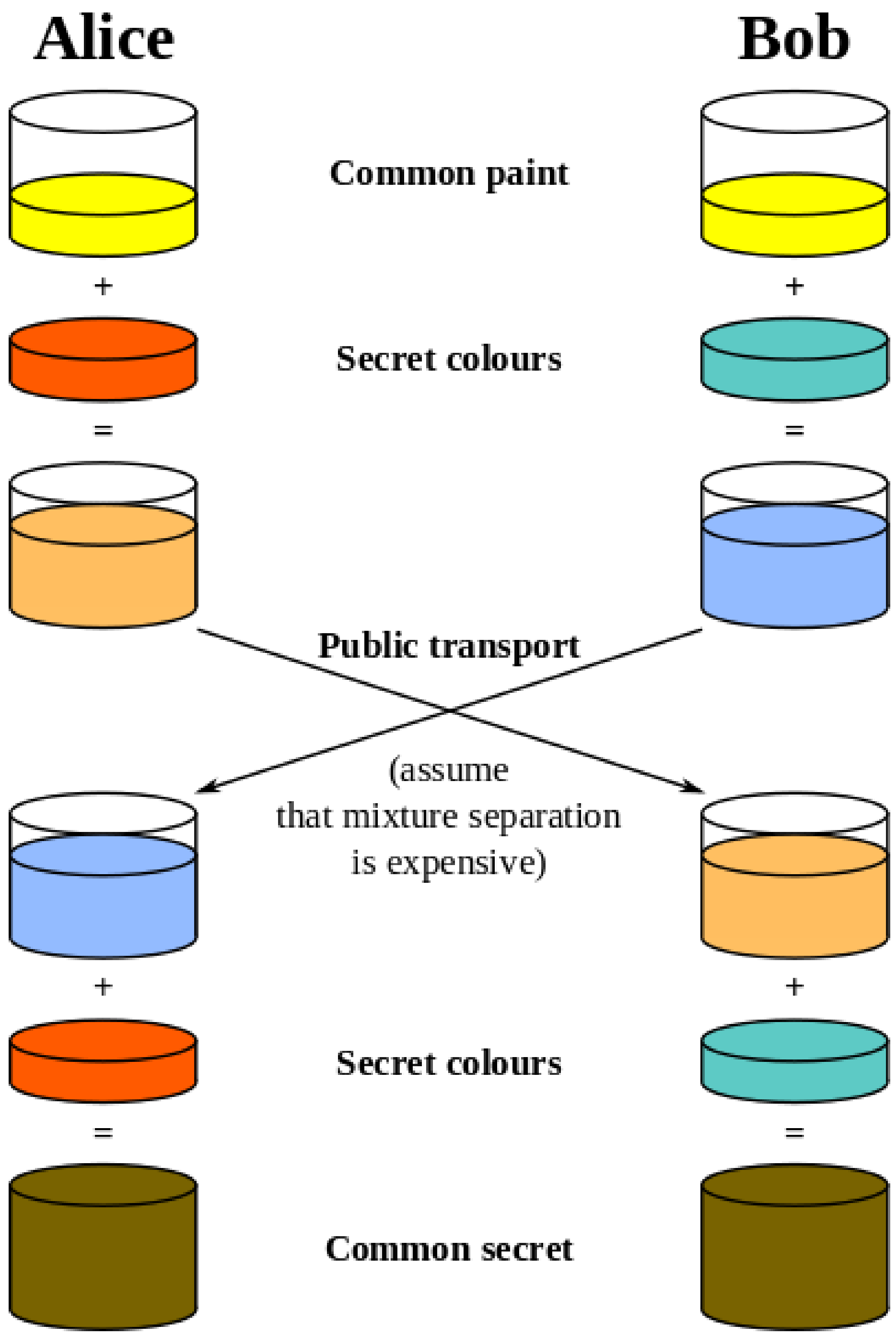
# Diffie-Hellman key exchange

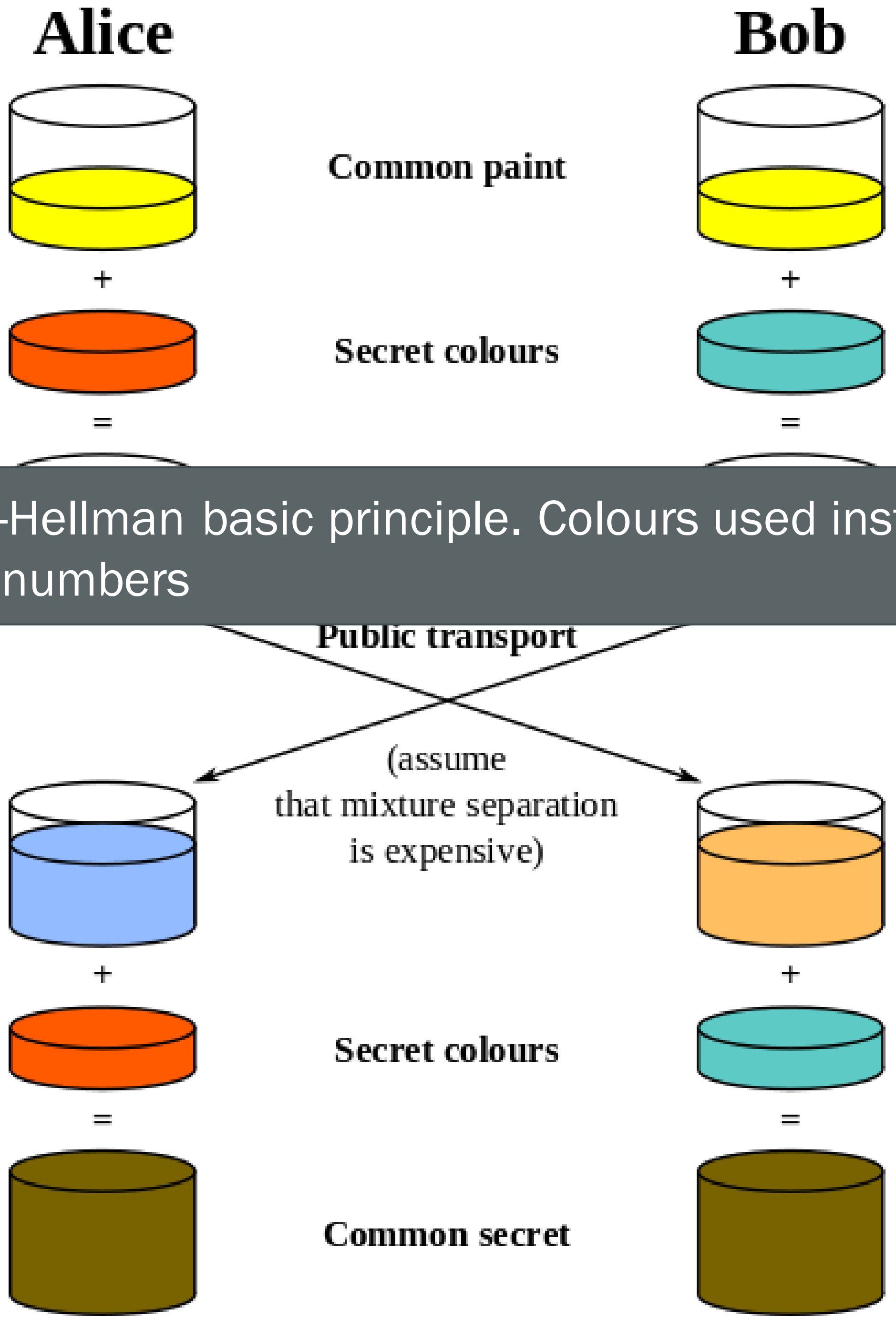


- Uses mathematical one-way functions
- Security
  - Brute f
- Mathema
- Different
  - DH Gro
  - DH Gro
  - DH Gro
- Higher gr

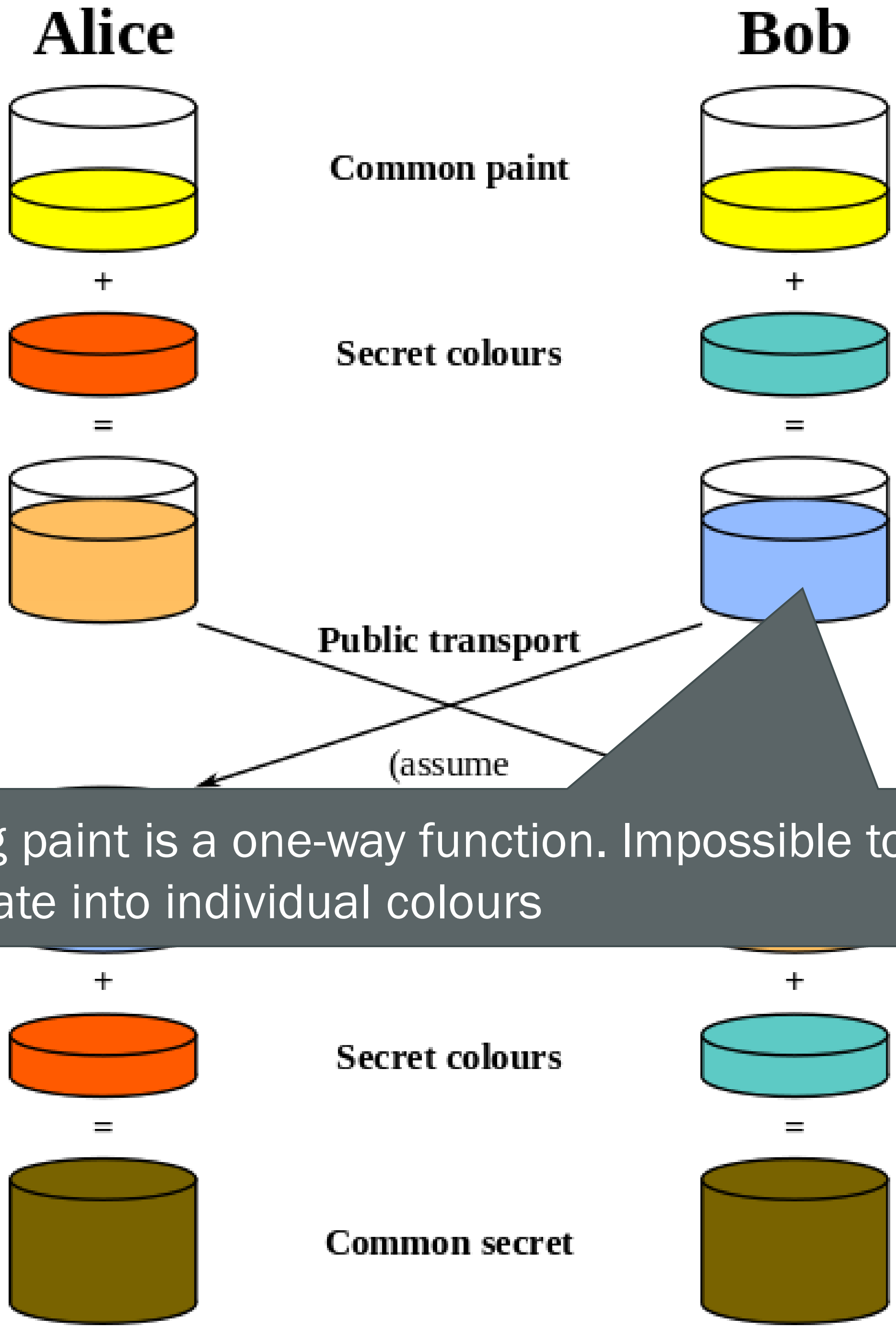
*A 1024 bit prime:*

179769313486231590770839156793787453197860296048756011706444423684197180216158519368947833795864925541502180565485980503646440548199239100050792877003355816639229553136239076508735759914822574862575007425302077447712589550957937778424442426617334727629299387668709205606050270810842907692932019128194467627007

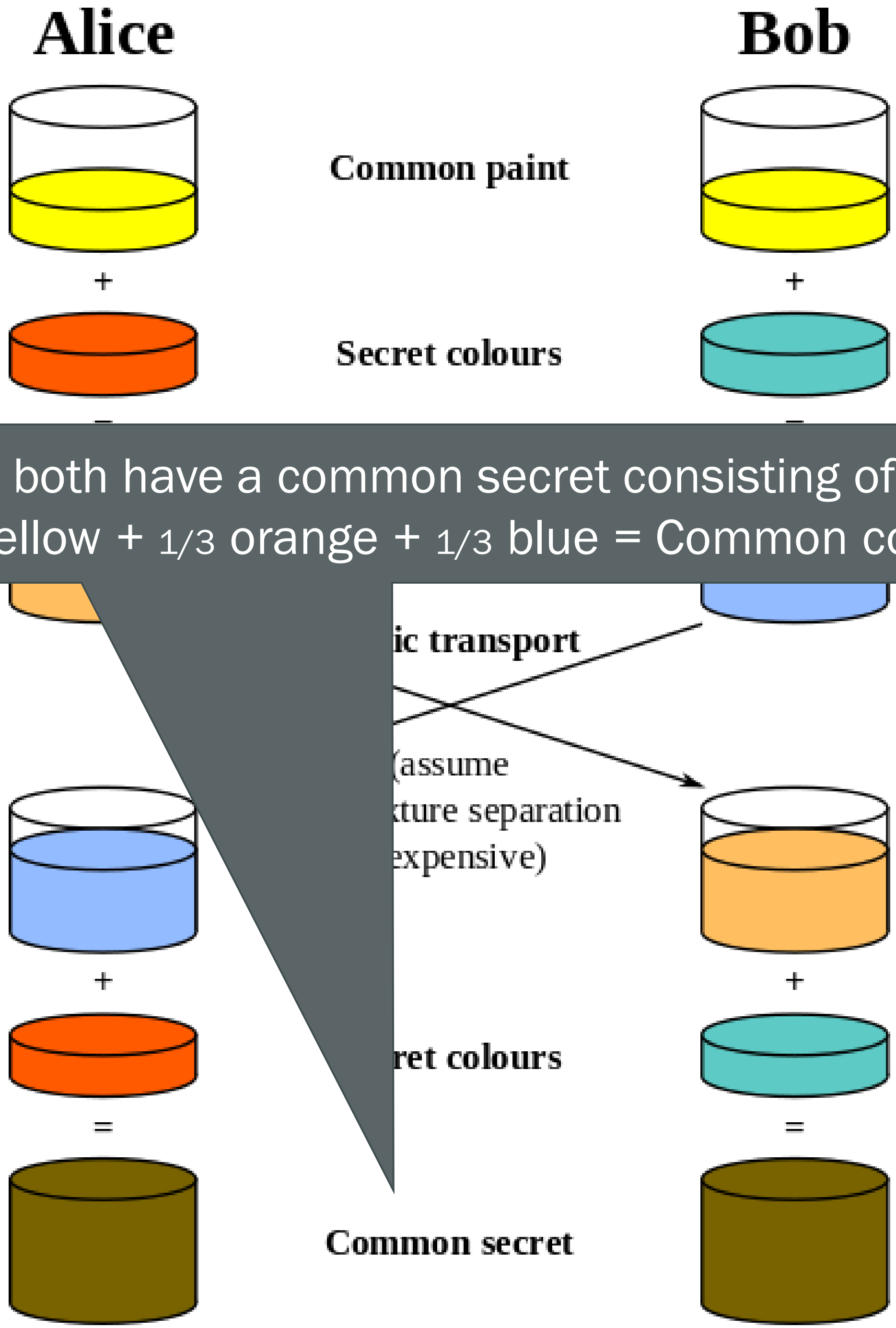

Alice
Bob
Common paint
+
Secret colours
=
Public transport
(assume
that mixture separation
is expensive)
+
Secret colours
=
Common secret




Diffie-Hellman basic principle. Colours used instead of huge numbers




Mixing paint is a one-way function. Impossible to separate into individual colours




They both have a common secret consisting of
1/3 yellow + 1/3 orange + 1/3 blue = Common colour

# hashes

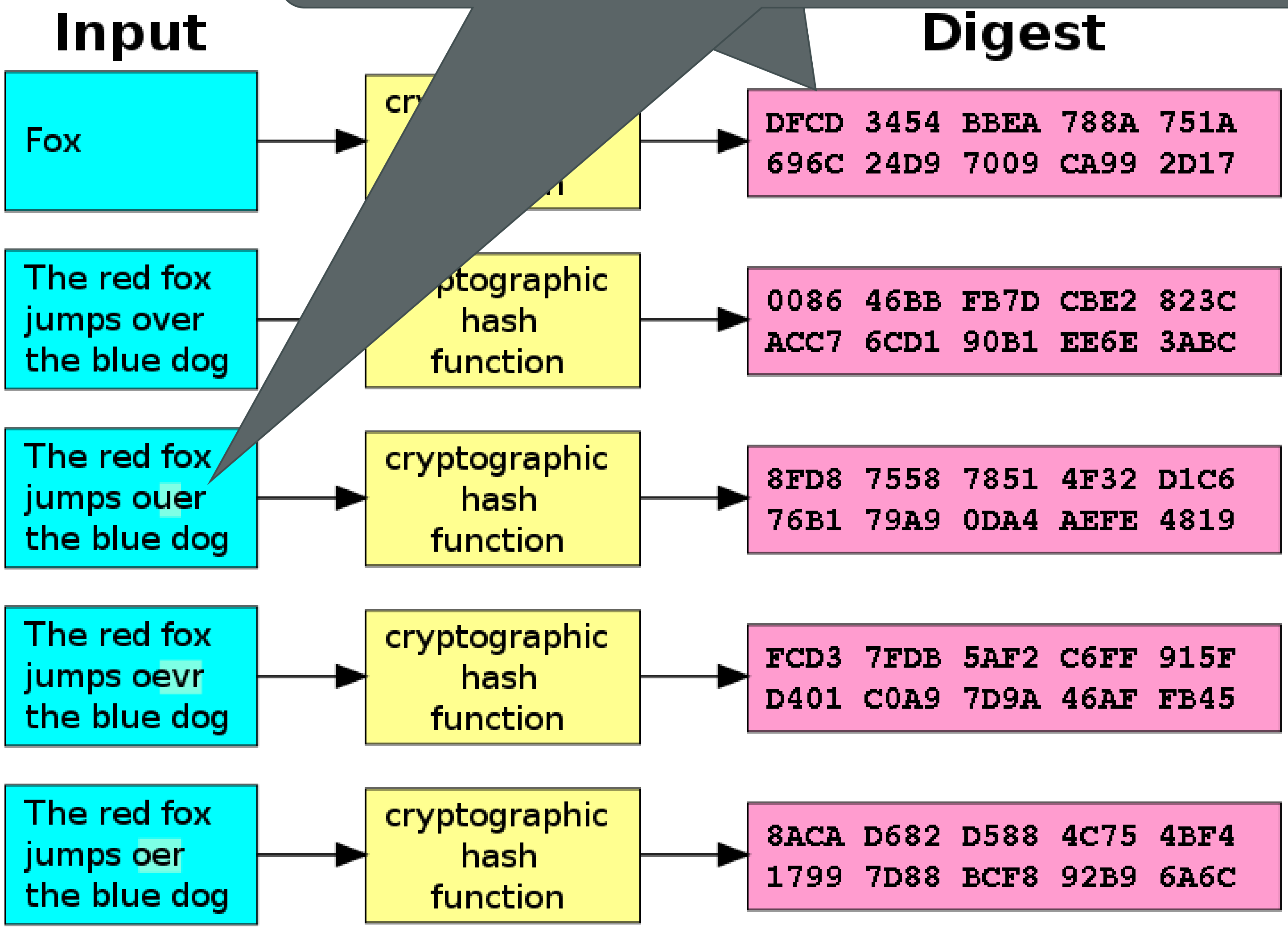
- A hash is a mathematical oneway function
- A digital fingerprint of a dataset
- Maps variable length data to fixed length data
- Used for example to protect passwords
- MD5 is still used
  - MD5 hash is considered compromised
  - Other hashes such as SHA-1, SHA-2 and SHA-3 are more secure. SHA-3 the most secure.

# Ha

Note the output of the hash function all have the same length – regardless of

The hash value is cal

A small change in the input value yields a totally different digest

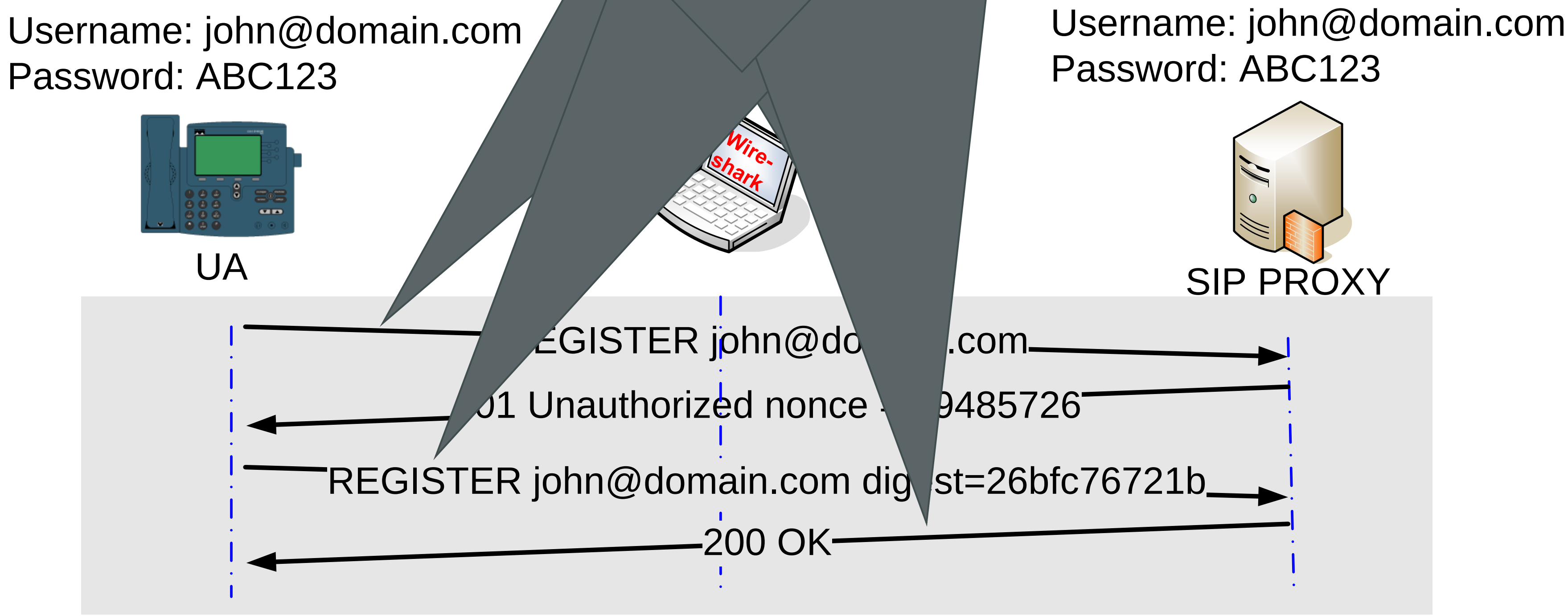


# Basic principle

Teknologisk videncenter – en del af mercantec

- The password are
  - The “hacker” capt

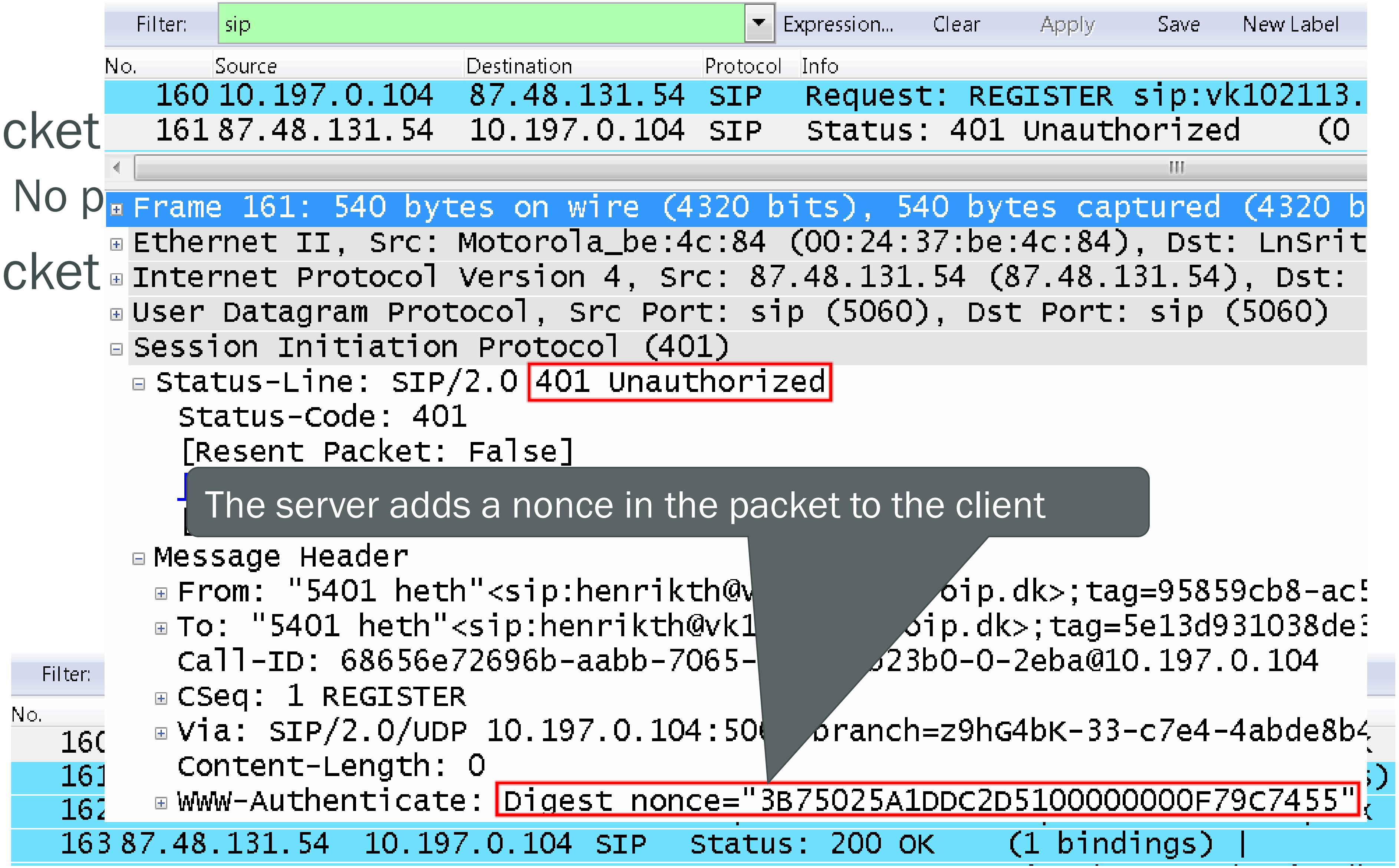
The hacker has learned
The username – the public URI
The nonce
The hash’ed password+nonce
Next time the server will choice a new random nonce



# Wireshark capture

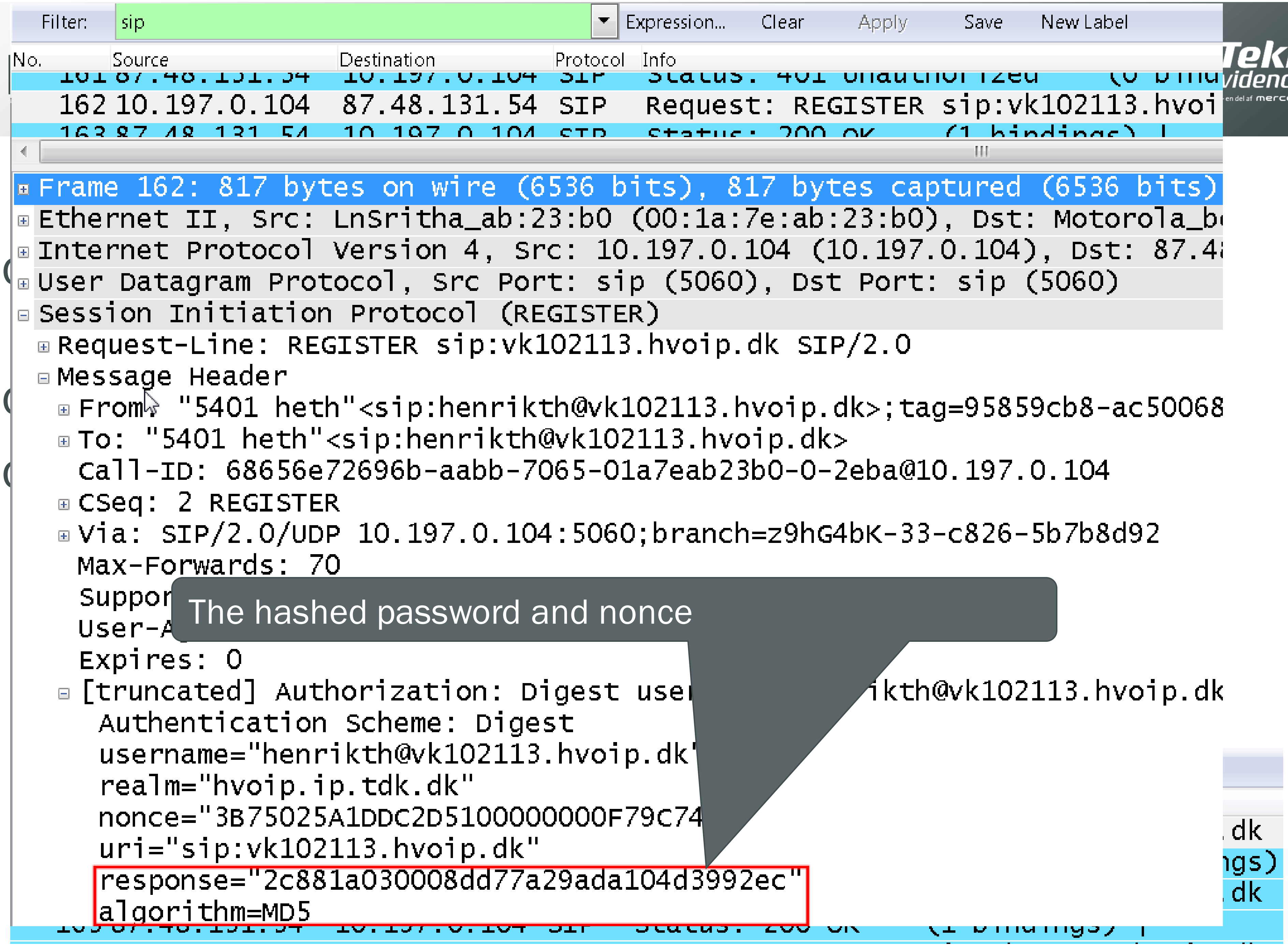
Teknologisk videncenter – en del af mercantec

- Packet
  - No p
- Packet



# Wi

- Pa
  - 
- Pa
- Pa
  - 




Teknologisk Videncenter

# Wireshark capture

Teknologisk videncenter – en del af mercantec

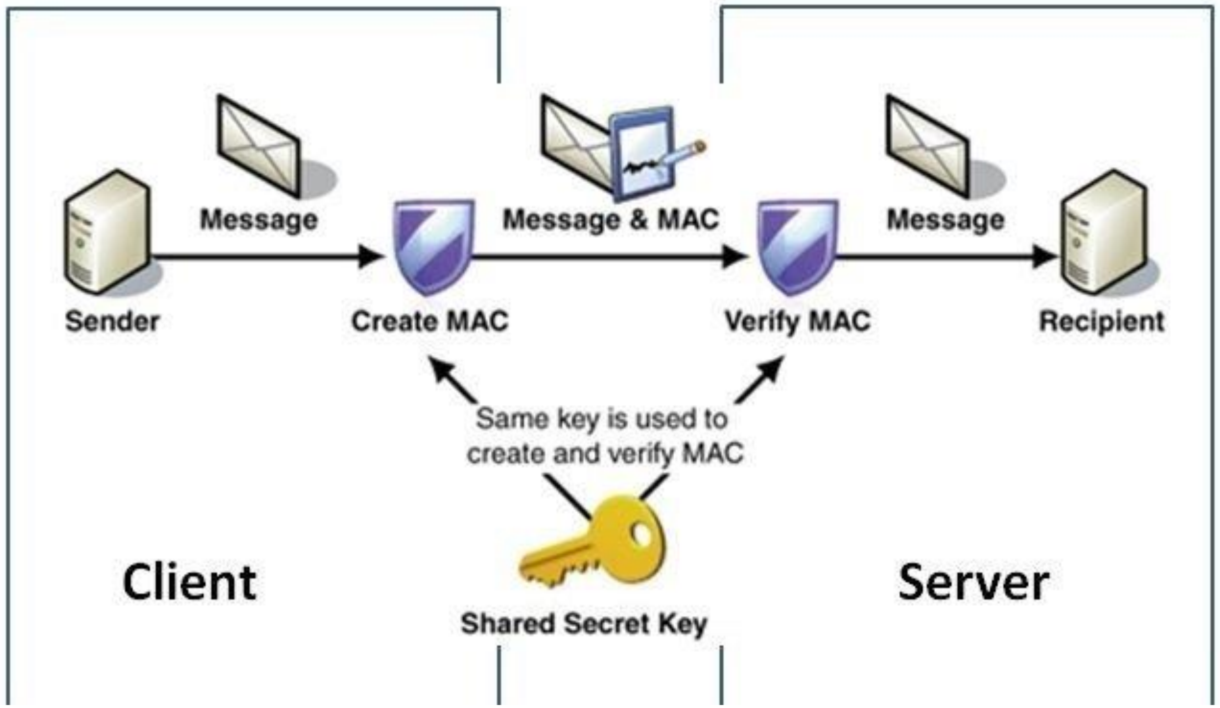
- Packet 160 – Client register request
  - No password attached
- Packet 161 – Register rejected
- Packet 162 – Client register request
  - Hash digest included
- Packet 163 – Server registers client
  - The client is online

Filter: sip   Expression... Clear Apply Save New Label

| No. | Source | Destination | Protocol | Info |
|---|---|---|---|---|
| 160 | 10.197.0.104 | 87.48.131.54 | SIP | Request: REGISTER sip:vk102113.hvoip.dk |
| 161 | 87.48.131.54 | 10.197.0.104 | SIP | Status: 401 Unauthorized (0 bindings) |
| 162 | 10.197.0.104 | 87.48.131.54 | SIP | Request: REGISTER sip:vk102113.hvoip.dk |
| 163 | 87.48.131.54 | 10.197.0.104 | SIP | Status: 200 OK (1 bindings) \| |

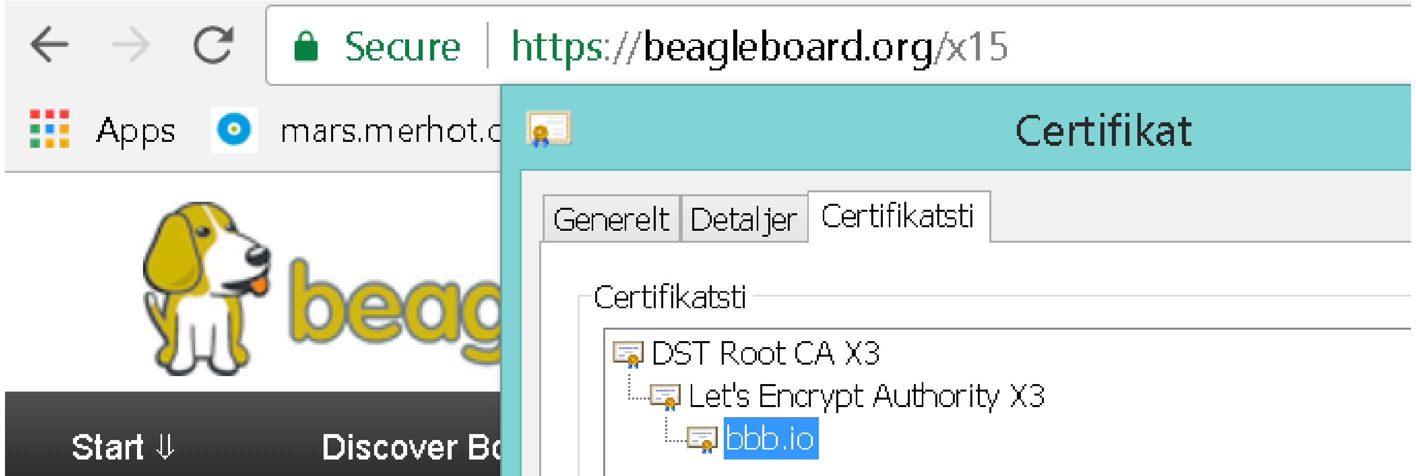
# HMAC

- *Hashed Message Authentication Code (HMAC)*
- *Includes a secret key in the hash calculation*
- *Eavesdropper cannot tamper with packets*



# Digital signatures

- A digital signature provides three benefits:
  - Authentication – Who you are
  - Data integrity – Data not tampered
  - Nonrepudiation – Proves that it is you. (You cant say it's not you)
- A digital certificate needs a trusted third party – a CA
- A Certificate Authority hands out digital certificates
  - Public key certification from CA ensures you trust the other party



# Key management

Teknologisk videncenter – en del af mercantec

- Key management deals with
  - Generating keys (Symmetric and assymmetric)
  - Verifying keys
  - Storing keys safely
  - Destroying keys after end-of-life
- Next-generation Encryption protocols
  - NSA suite A cryptography – Classified algorithms (Wikipedia link)
  - NSA suite B cryptography – Public algorithms (Wikipedia link)

# IPsec and TLS/SSL

Teknologisk videncenter – en del af mercantec

- IPsec is a suite of protocols used to protect IP packets for decades
  - Used for both remote-access and Site-to-Site VPN's
  - Both parties would need a PSK – Preshared Key or a CA digital certificate
- TLS/SSL – Transport Layer security/Secure Socket Layer
  - SSL was developed by Netscape – First version in 1995
  - TLS version 1 was introduced as a new version of SSL version 3 in 1999
  - TLS/SSL is used to make HTTPS: connections
  - To make a secure connection only one party needs a digital certificate
- SSL server test (Link) - https://globalsign.ssllabs.com/

# VPN technologies review

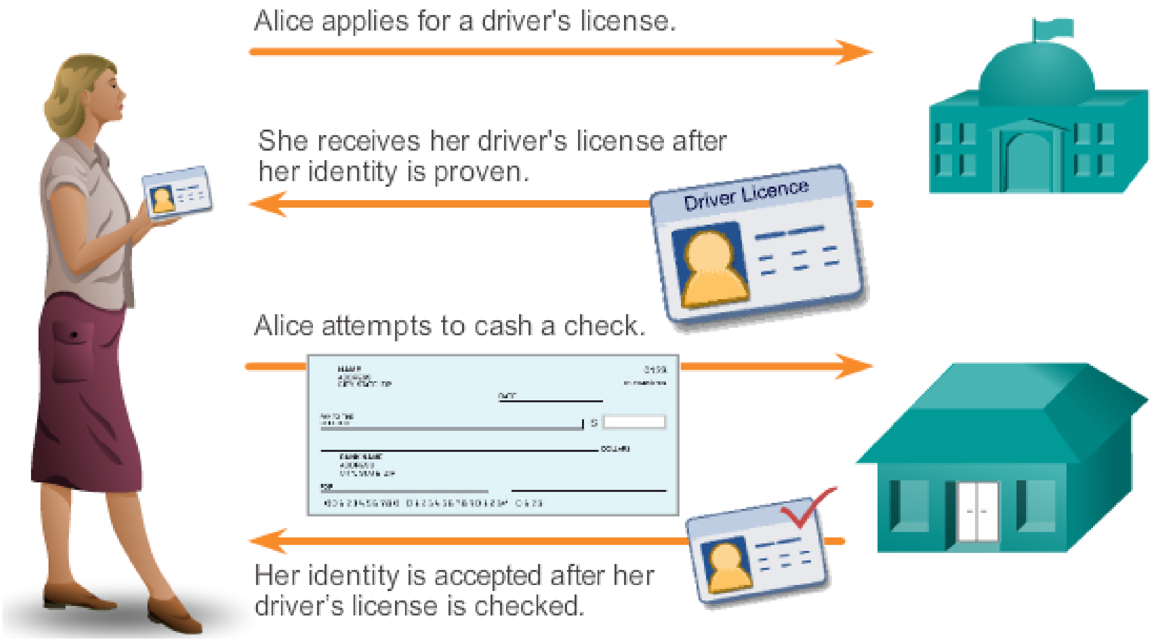
Teknologisk videncenter – en del af mercantec

| Component | Function | Examples of Use |
|---|---|---|
| Symmetrical encryption algorithms | Use the same key for encrypting and decrypting data. | DES, 3DES, AES, IDEA |
| Asymmetrical encryption | Uses a public and private key. One key encrypts the data, and the other key in the pair is used to decrypt. | RSA, Diffie-Hellman |
| Digital signature | Encryption of hash using private key, and decryption of hash with the sender's public key. | RSA signatures |
| Diffie-Hellman key exchange | Uses a public-private key pair asymmetrical algorithm, but creates final shared secrets (keys) that are then used by symmetrical algorithms. | Used as one of the many services of IPsec |
| Confidentiality | Encryption algorithms provide this by turning clear text into cipher text. | DES, 3DES, AES, RSA, IDEA |
| Data integrity | Validates data by comparing hash values. | MD5, SHA-1 |
| Authentication | Verifies the peer's identity to the other peer. | PSKs, RSA signatures |

# PKI – Public Key Infrastructure

- This section covers the moving parts and pieces involved with the public key infrastructure

**Driver License PKI Analogy**



# Public and Private Key Pairs

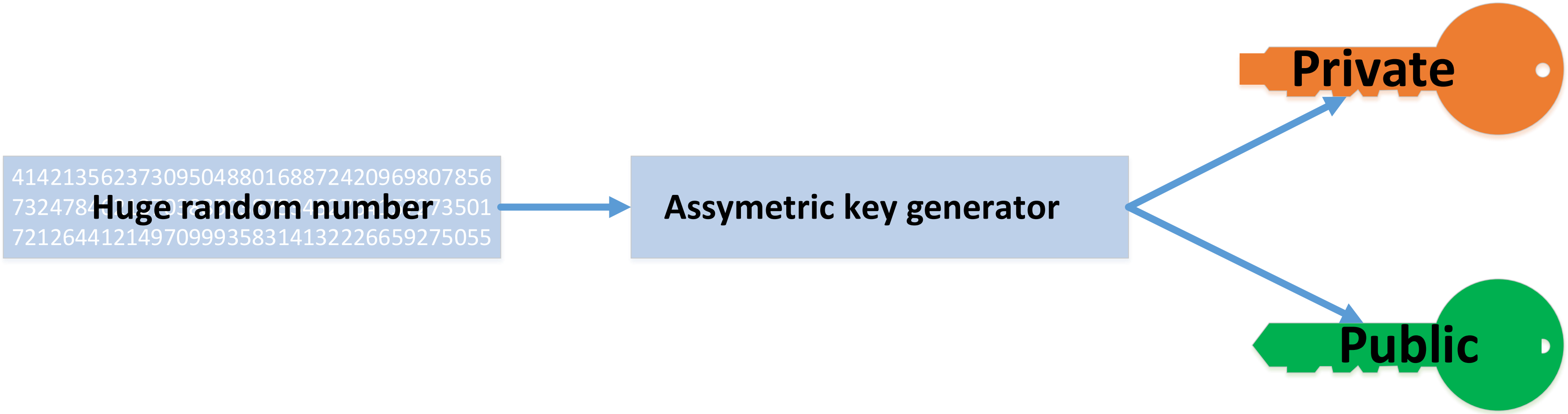
Teknologisk videncenter – en del af mercantec

- A *key pair* is a set of two keys that work in combination with each other as a team
- For example, the private key for a web server is known only to that specific web server
- The public key – is well public
- Data encrypted with the public key can only be decrypted with the web servers private key
- This is called:
  - *public key cryptography* or *asymmetric key cryptography*

# Public and Private Key Pairs

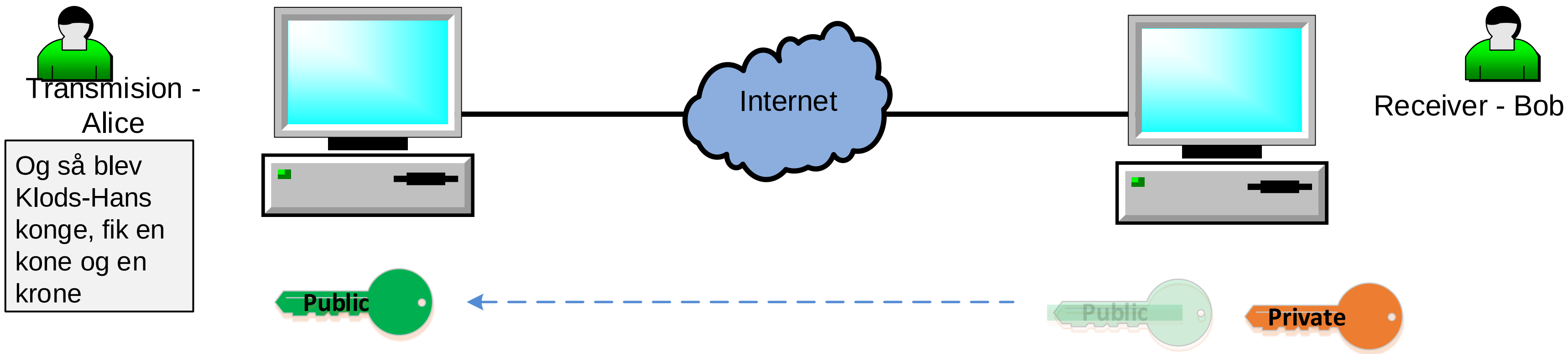
Teknologisk videncenter – en del af mercantec

- Key generation process



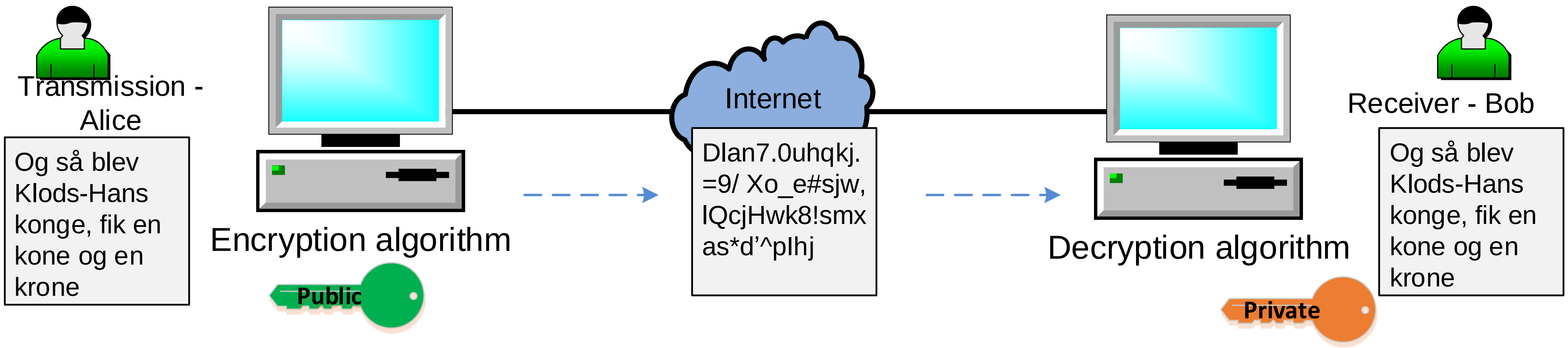
# Asymmetric key distribution

- Bob distributes his public key to Alice
  - Anybody could intercept his key



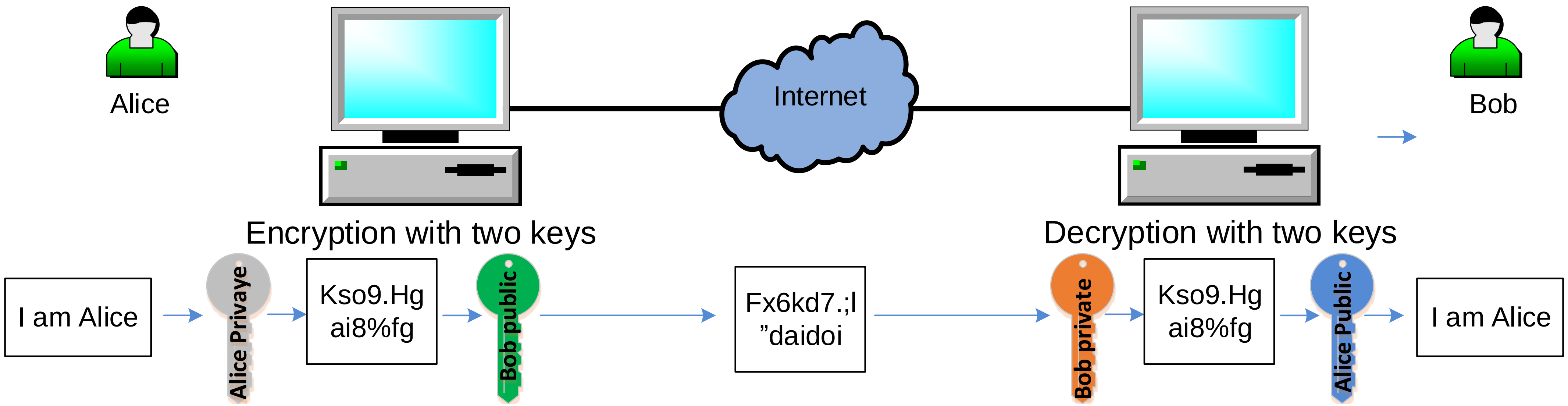
# Asymmetric key en/de-cryption

- Using the public key – Alice encrypts the secret message
- The only key that can decrypt the message is Bob's private key
  - What's encrypted with the public key can only be decrypted with the private
  - What's encrypted with the private key can only be decrypted with the public



# Asymmetric key for identity

- If bob from a trusted third party got Alice’s public key Alice and
- Alice proves she has the private key – Bob know he is talking to Alice



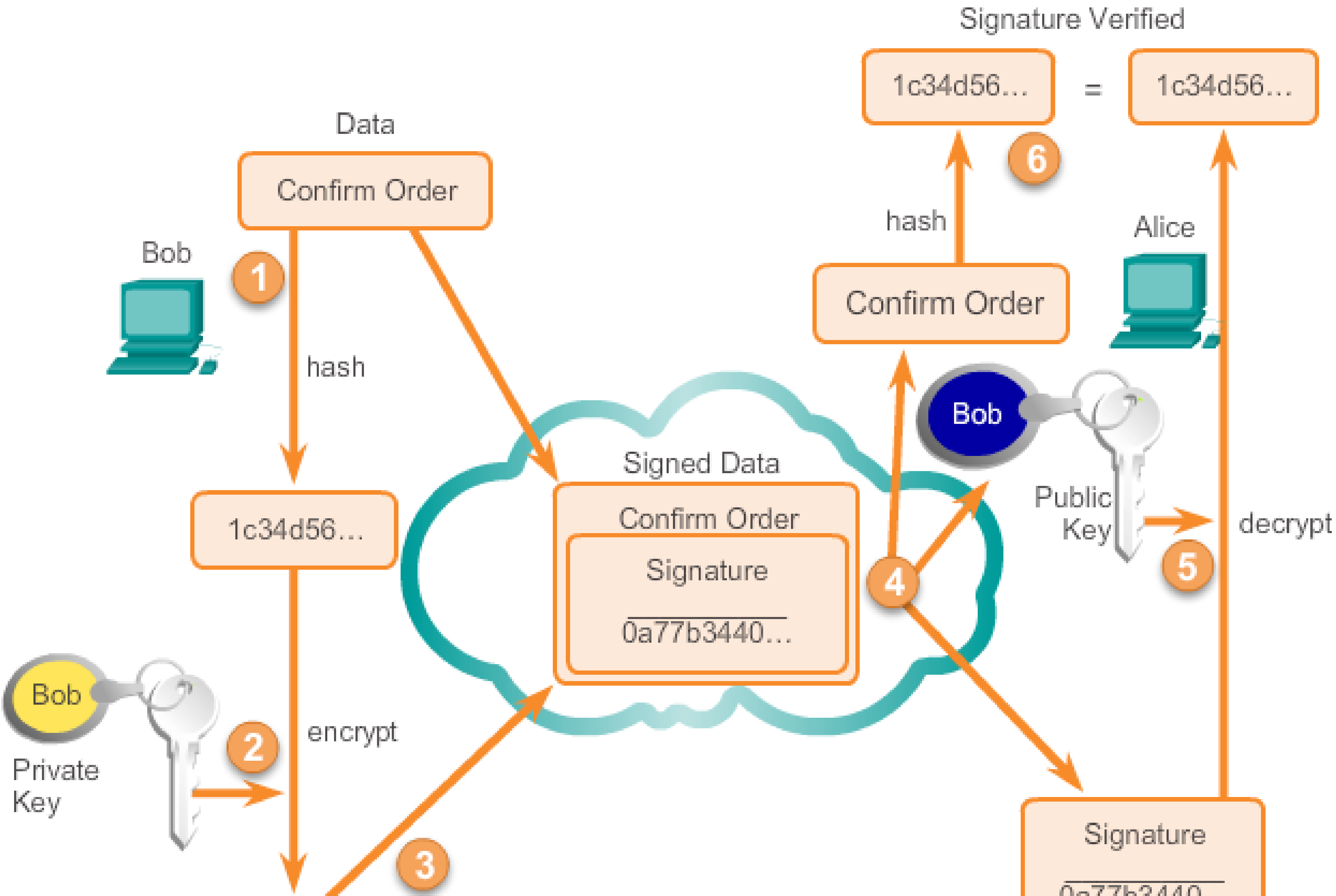
# RSA algorithm keys and certificates

- Bob and Alice each generate their own key-pair
- They enroll with a CA (Certificate Authority)
  - The CA know the IP addresses, names and public keys of Bob and Alice
  - The CA generate and send Digital Certificates to Bob and Alice
  - The CA signes Bob and Alices Digital Certificates – authenticating them
- When Bob and Alice want to authenticate each other they
  - Send their Digital Certificate to the other party
  - They verify  the authenticity of the certificate by checking the signature of a CA

# Creating a Digital Certificate

- Bob takes some data and
  - Generate a hash from the data
  - Encrypts the hash with his private key
  - Transmit the data and the encrypted hash in an encrypted packet
- Alice receives the data and the encrypted hash
  - Alice's computer obtains Bob's public key from the CA (www.bob.dk)
  - Alice decrypts the hash with Bob's public key
  - Alice generate a hash from the data
  - If Bob's hash and Alice's hash are equal – Bob has proved his identity

# Digital Signature Process



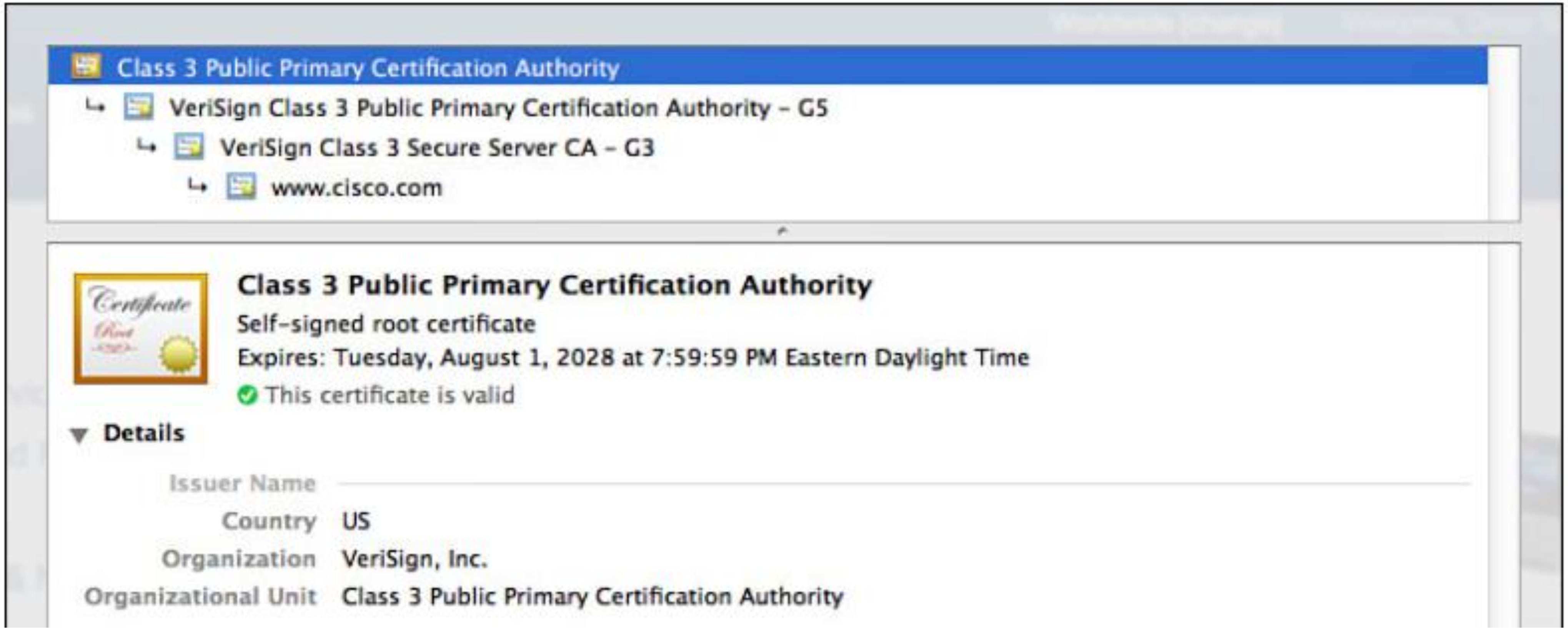
# Certificate Authority - CA

Teknologisk videncenter – en del af mercantec

- A CA is a computer or entity that generates and issues digital certificates.
- Inside the certificate is information about the identity of a device
- Such as
  - fully qualified domain name (FQDN) - fx. www.Mercantec.dk
  - Public key

# Root Certificate

- A root certificate contains the public key of the CA server

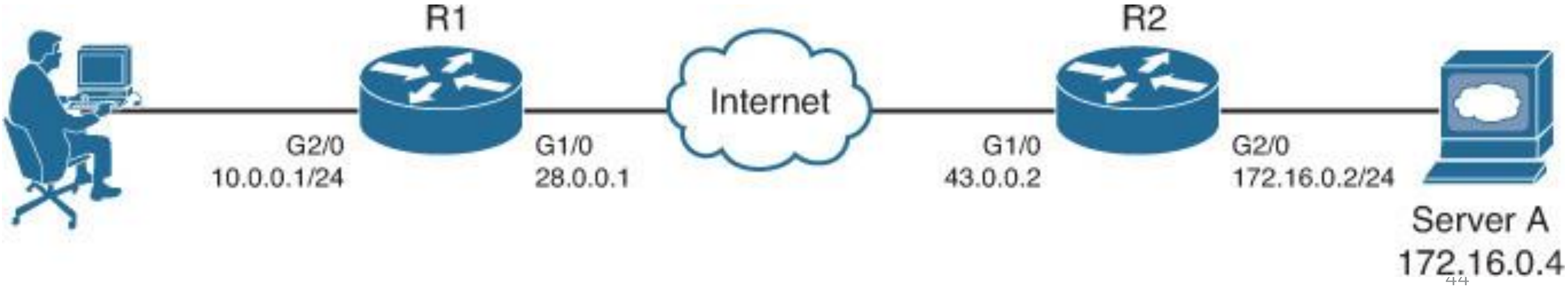


# Chapter 6

Fundamentals of IP security

# The goal of IPsec

| Goal | Method That Provides the Feature |
|---|---|
| Confidentiality | Encryption |
| Data integrity | Hashing |
| Peer authentication | Pre-shared keys, RSA digital signatures |
| Antireplay | Integrated into IPsec, basically applying serial numbers to packets |



# The goal of IPsec

Teknologisk videncenter – en del af mercantec

- **Confidentiality:**
  - Provided through encryption changing clear text into cipher text.
- **Data integrity:**
  - Provided through hashing and/or through *Hashed Message Authentication Code (HMAC)*
- **Authentication:**
  - Provided through authenticating the VPN peers near the beginning of a VPN session using *pre-shared keys (PSK)* or digital signatures
- **Antireplay protection:**
  - When VPNs are established, the peers can sequentially number the packets

# Internet Key Exchange (IKE) Protocol

Teknologisk videncenter – en del af mercantec

- IPsec uses the *Internet Key Exchange (IKE)* protocol to negotiate and establish secured site-to-site or remote access *virtual private network (VPN)* tunnels
- IKE is a framework provided by the *Internet Security Association and Key Management Protocol (ISAKMP)*
- In IKE Phase 1 IPsec peers negotiate and authenticate each other.
- In Phase 2 they negotiate keying materials and algorithms for the encryption of the data being transferred over the IPsec tunnel.

# Internet Key Exchange (IKE) Protocol

Teknologisk videncenter – en del af mercantec

- There are two versions of IKE:
  - **IKEv1:** Defined in RFC 2409, *The Internet Key Exchange*
  - **IKE version 2 (IKEv2):** Defined in RFC 4306, *Internet Key Exchange (IKEv2) Protocol*
- IKEv2 enhances the function of performing dynamic key exchange and peer authentication

# IPsec

- IPsec is standardized and not properatary. (Cisco)
- IPsec er scalable and can be used from small to huge networks

# Abbrevations

Teknologisk videncenter – en del af mercantec

- ISAKMP (Internet Security and Key Management Protocol)
  - Establish , negociate connections
- SA (Security Association)
  - The secure partner in the other end of the VPN connection
- RSA (Rivest, Shamir og Adleman)
  - Assymetric encryption algorithm
- CA (Certificate Authority)
  - Digital signature provider

# Agenda og forkortelser

Teknologisk videncenter – en del af mercantec

- IPsec protocols
  - IKE (Internet Key Exchange)
  - ESP (Encapsulating Security Payload)
  - AH (Authentication Header)
- IPsec encryption
  - DES (Data Encryption Standard)
  - 3DES (Triple Data Encryption Standard)
  - AES (Advanced Encryption Standard)
- HASH: Digital fingerprint
  - HMAC (Hash-based Message Authentication Code)
  - MD5 (Message Digest 5)
  - SHA (Secure Hash Algorithm)

# IPsec overview

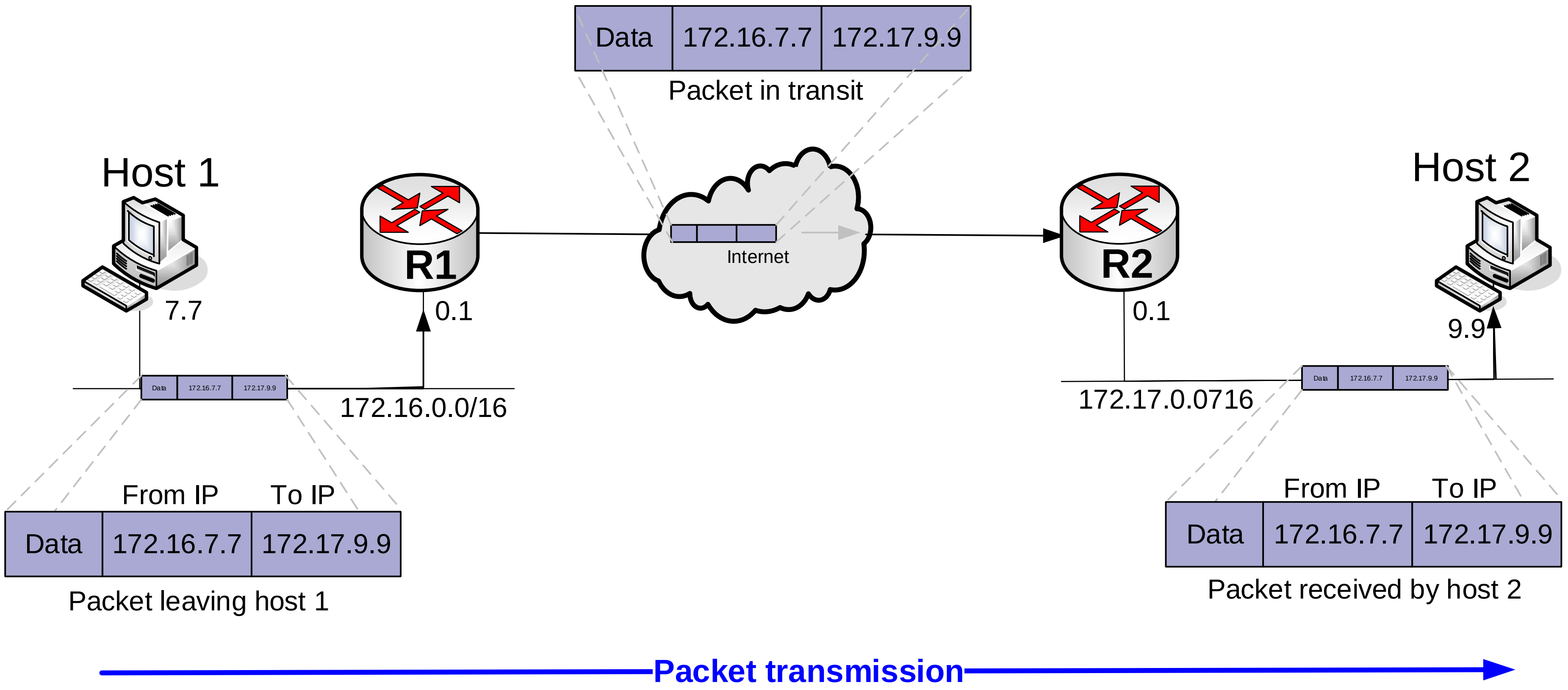
Teknologisk videncenter – en del af mercantec

- Data Confidentiality – (option i IPsec)
  - Kryptering af data i transit.
  - Krypteringsalgoritmer i ESP: DES, 3DES, AES
- Data Integrity – (Mandatory i IPsec)
  - Data er ikke ændret i transit.
  - HASH værdi: MD5, SHA
- Data origin authentification (Mandatory i IPsec)
  - Sikkerhed for partners identitet
  - Identifikation: RSA signatur eller Preshared-key
- Anti replay – (Option i IPsec)
  - Man kan ikke ’optage’ og gentransmitere en transaktion.
  - Sekvensnumre i pakkerne skal passe.

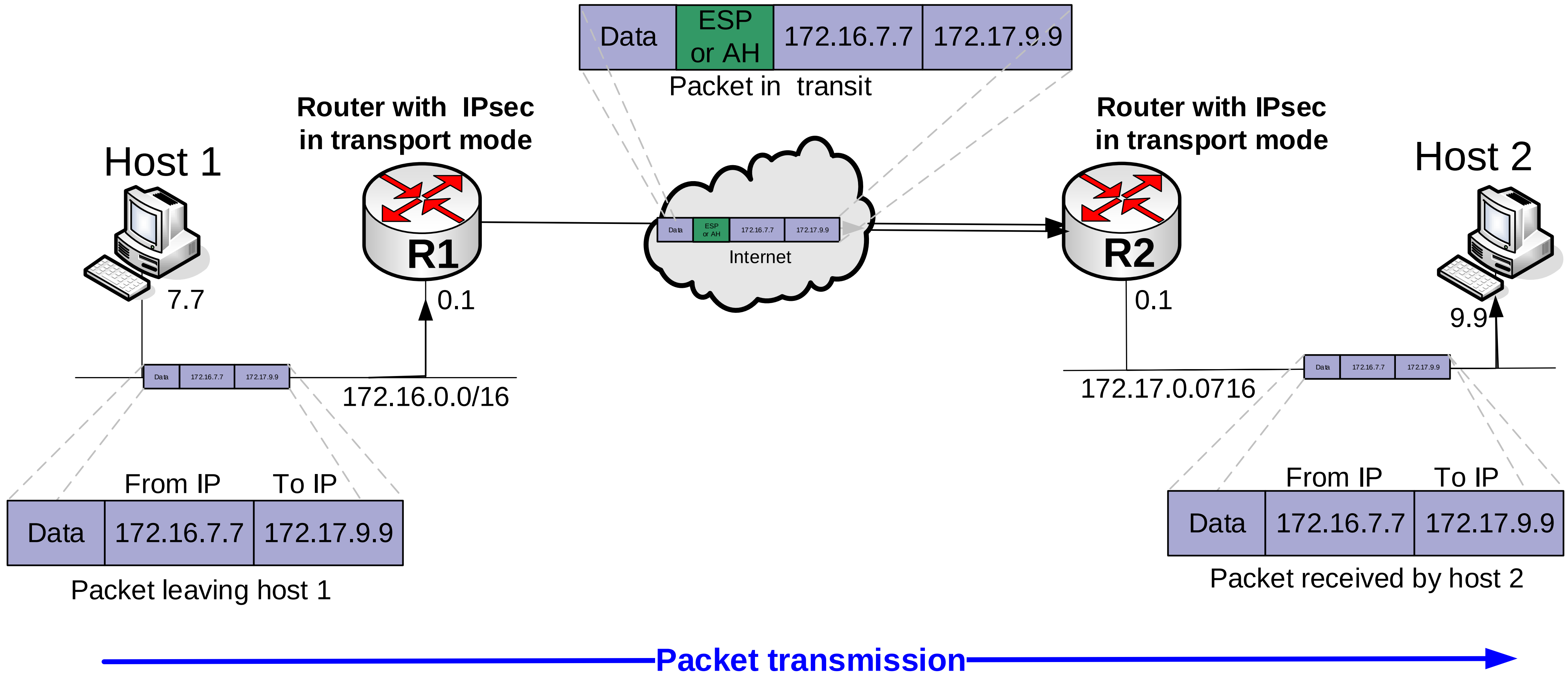
# IPsec overblik

- IKE (Internet Key Exchange)
  - Exchange of keys and security parameters
- ESP (Encapsulating Security Payload)
  - Can secure
    - Confidentiality (Encryption)
    - Integrity (data not changed in transit)
    - Authentication ( Identity of transmitter)
    - Anti-replay (Data can’t be retransmitted. (Sequence numbers))
- AH (Authentication Header)
  - Can secure
    - Integrity (data not changed in transit)
    - Authentication ( Identity of transmitter)
    - Anti-replay (Data can’t be retransmitted. (Sequence numbers))
  - Cant secure
    - Confidentiality (Encryption)

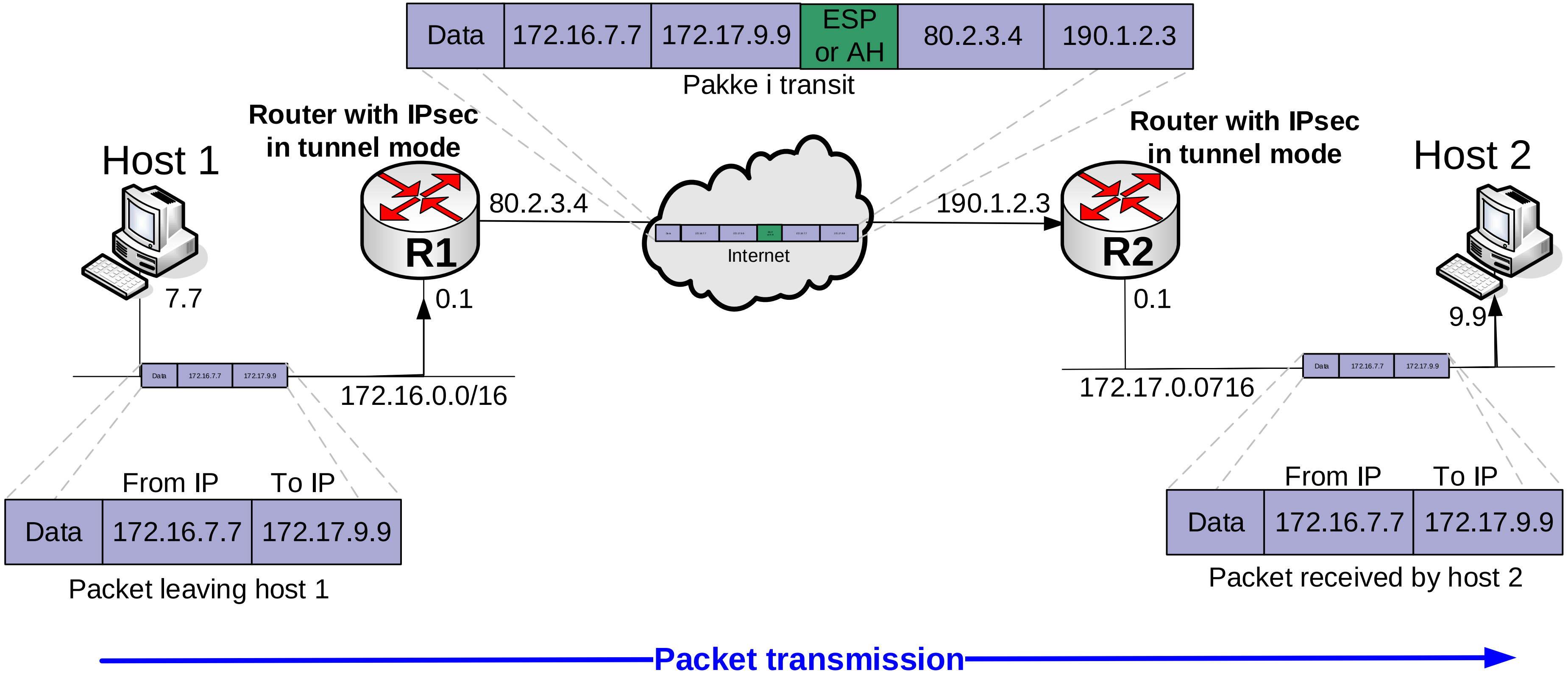
# Principle: Normal Routning



# Principle: IPsec Transport Mode



# Principle: IPsec Tunnel Mode



# IPsec modes

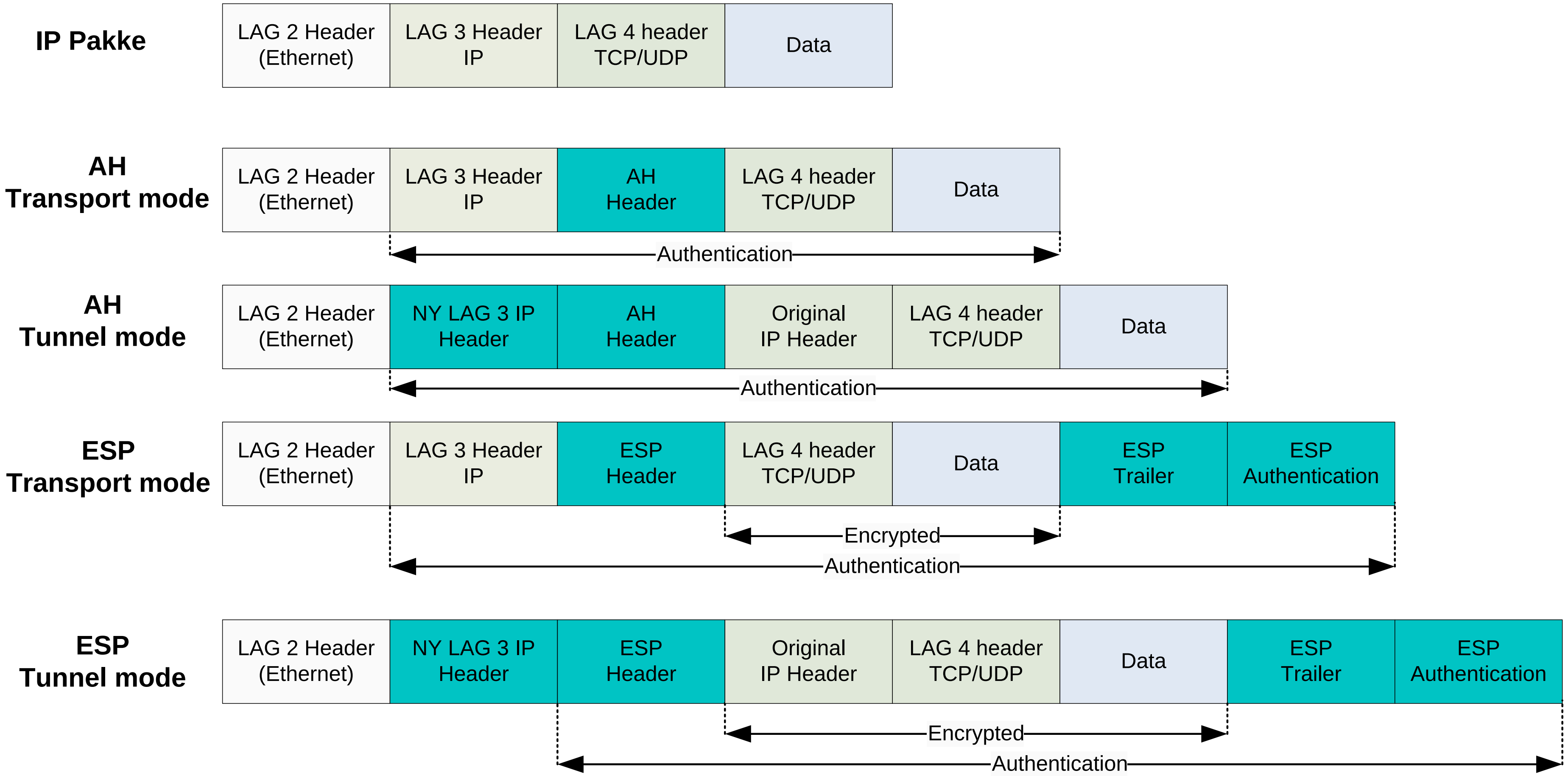
- Transport mode
  - Secures from OSI layer 4 with ESP or AH

| | | | | |
|---|---|---|---|---|
| LAG 2 Header (Ethernet) | LAG 3 Header IP | ESP eller AH | LAG 4 header TCP/UDP | Data |

- Tunnel mode
  - Secures from OSI layer 3 with ESP or AH

| | | | | | |
|---|---|---|---|---|---|
| LAG 2 Header (Fx Ethernet) | Ny IP Header | ESP eller AH | IP Header | TCP/UDP Header | Data |

# IPsec Headers




Teknologisk videncenter – en del af mercantec

# Chapter 7

Implementing Ipsec Site-to-Site VPNs

# Peer Authentication

- Identification of parters in a communication channel
  - Username and password
  - One-Time-Password (OTP)
  - Biometrics
  - Preshared keys
  - Digital certificate (Digital signature)

# ISAKMP

- Internet Security Association and Key Management Protocol
- SAKMP is a procedure that defines how exchange of keys is done and what security policy used
- ISAKMP defines procedures to:
  - Establish, negociate, change and delete SA'es
    - SA = Security Associations or IPsec end poins
- ISAKMP uses the protocols defined in IKE

# IKE - Internet Key Exchange

Teknologisk videncenter – en del af mercantec

- The IKE protocol is used to exchange IPsec parameters and keys between the two VPN parties
- IKE tries to establish a Security Association (SA) between the two
- IKE uses the following protocols to perform Authentication and key exchange
  - ISAKMP
  - OAKLEY

# IKE

- Internet Key Exchange
- Is a hybrid protocol used by ISAKMP
- Before any data can be exchanged IKE will
  - Exchange keys
  - Identify the other party
    - Preshared Keys
    - Digital Signatur (CA – Certificate Authority)

# Configuration of IPsec

1. Configure ISAKMP
   - Choice policy/policies
     - Preshared Keys
     - Digital certificat
2. Configure IPsec
3. Create a Crypto map
4. Put the crypto map on a interface
5. One end of the VPN is ready

# ISAKMP: Configuration of Preshared-Keys

Teknologisk videncenter – en del af mercantec

- Define one or more ISAKMP Policy Objects

```
R2(config)# crypto isakmp policy 1
```

- Which Diffie-Hellmann group to use
  - Group 1: 768 bit (default)
  - Group 2: 1024 bit
  - Group 5: 1536 bit

```
R2(config-isakmp)# group 2
```

- What HASH type to use
  - MD5: 128 bit
  - SHA-1: 160 bit.
  - SHA-1 More secure

```
R2(config-isakmp)# hash md5
```

# ISAKMP: Configuration of Preshared-Keys

Teknologisk videncenter – en del af mercantec

- Lifetime of a SA (Security Association) before renegociation
  - Default: 86400 sekunder (en dag)

```
R2(config-isakmp)# lifetime 500
```

- How to identify the other party
  – Authentication

```
R2(config-isakmp)# authentication pre-share
```

- Who is the other party and how to identify
  – Key 0: un-encrypted password
  – Key 6: encrypted password

```
R2(config-isakmp)# exit
R2(config)# crypto isakmp key 0 18heise address 192.168.2.1
```

# ISAKMP: Configuration of Preshared-Keys

- The full IKE configuration of preshared keys

```
R2(config)# show run
crypto isakmp policy 1
  hash md5
  authentication pre-share
  group 2
  lifetime 500
crypto isakmp key 0 l8heise address 192.168.2.1
```

# ISAKMP: Configuration of Preshared-Keys

- Create an ACL

```
R2(config)# access-list 101 permit ip 192.168.3.0 0.0.0.255 172.16.4.0 0.0.255.255
```

- Create one or more IPsec transform sets
  - Mode tunnel (default)
  - Mode transport

```
R2(config)# crypto ipsec transform-set Kunde1 esp-sha-hmac esp-aes
R2(config-crypto-trans)# mode tunnel
R2(config-crypto-trans)# exit
R2(config)# crypto ipsec transform-set Kunde2 ah-md5-hmac
R2(config-crypto-trans)# mode tunnel
R2(config-crypto-trans)# exit
```

# IPsec: Create a crypto map

- Create one or more IPsec transform sets

```
R2(config)# cryto map Viborg 10 ipsec-isakmp
R2(config-crypto-map)# set peer 192.168.2.1
R2(config-crypto-map)# set transform-set Kunde1 Kunde2
R2(config-crypto-map)# match address 101
```

- Put on a interface to start

```
R2(config)# interface fastethernet0/1
R2(config-if)# crypto-map Viborg
```

# Full configuration

Teknologisk videncenter – en del af mercantec

```
R2(config)# show run
crypto isakmp policy 1
 hash md5
 authentication pre-share
 group 2
 lifetime 500
crypto isakmp key l8heise address 192.168.2.1
!
crypto ipsec transform-set Kunde1 esp-aes esp-sha-hmac
crypto ipsec transform-set Kunde2 ah-md5-hmac
!
crypto map Viborg 10 ipsec-isakmp
 set peer 192.168.10.38
 set peer 192.168.2.1
 set transform-set Kunde1 Kunde2
 match address 101
!
interface FastEthernet0/1
 ip address 192.168.71.1 255.255.255.0
 crypto map Viborg
!
access-list 101 permit ip 192.168.3.0 0.0.0.255 172.16.4.0 0.0.255.255
```

# Ipsec over GRE

- IPsec only transports IP unicast traffic - not Multicast.
- To transport multicast traffic from for example a routing protocol it can be tunneled through GRE first.