William Stallings
Data and Computer Communications
7th Edition

Bab 21

Keamanan jaringan

Hal yang dibutuhkan dlm keamanan

- Dapat dipercaya
- Berintegritas
- Tersedia

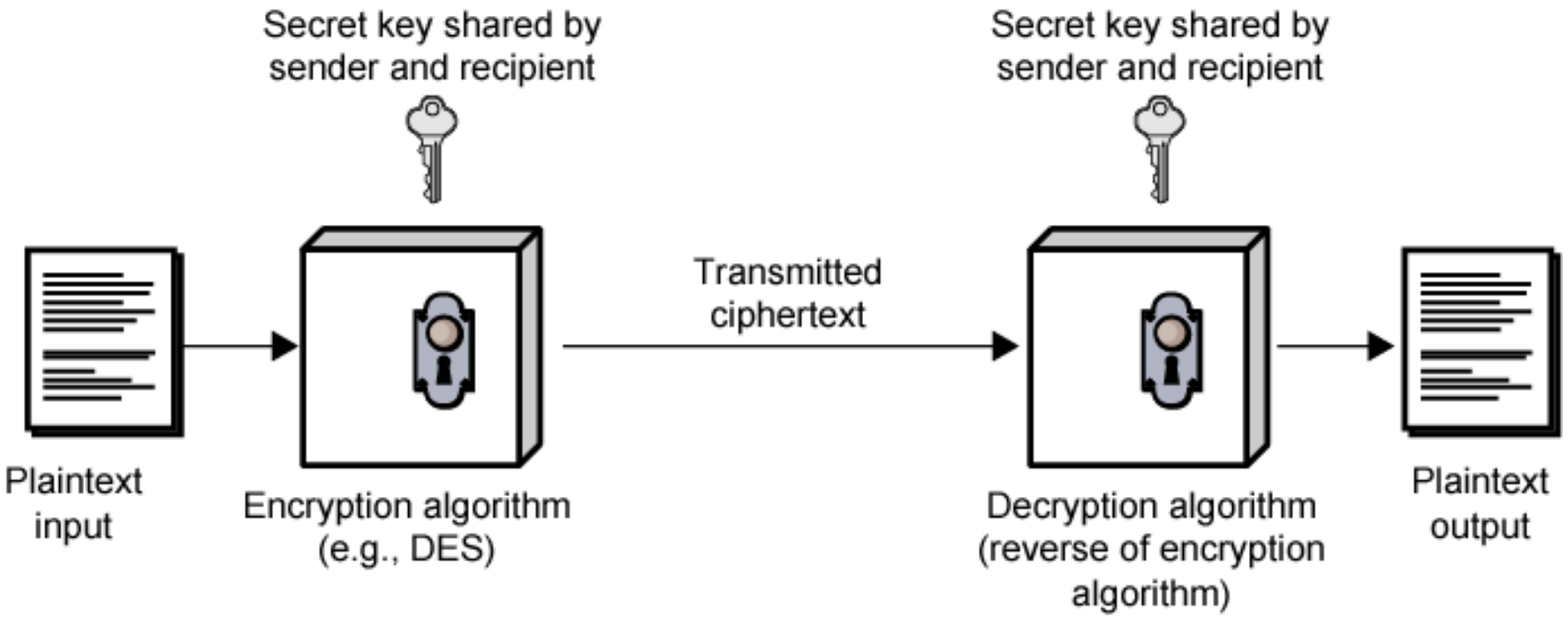
Menyerang pasif

- Tidak terdengar dalam transmisi
- Untuk memperoleh information
- Pelepasan dari isi surat
  - —Orang luar belajar isi dari transmisi.
- Analisa
  - —Dengan menangkap frekuensi dan panjang gelombang dari pesan ,enkripsi sama,komunikasi alami mungkin terkira.
- Sulit untuk deteksi
- Dapat dicegah

Active Attacks

- Penyamaran
  - —pemberlakuan menjadi sebuah kesatuan yang berbeda
- Mengulangi
- Modifikasi pesan
- Denial of pelayanan
- Mudah dideteksi
  - —Deteksi mudah untuk pencegahan
- Melindungi

Enkripsi Simetris(sederhana)



Komposisi

- Text datar
- Algoratima Enkripsi
- Kunci rahasia
- Text Rahasia
- Algoritma deskripsi

Requirements for Security

- Algoritma enkripsi kuat
  - —Sama jika diketauhi, sebaiknya tidak dapat untuk dekripsi atau percobaan kunci
  - —Sama jika sejumlah kepingan text merupakan tersedia bersama dengan text sederhana
- Pengirim dan Penerima harus memperoleh kerahasiaan kunci keamanan
- Salah satu kunci yang diketahui, semua komunikasi menggunakan kunci ini untuk bisa membaca

Penyerangan enkripsi

- Analisa kript
  - Menyampaikan secara alami dari algoritma ditambah beberapa pengetahuan karakteristik dari text sederhana.
  - Mencoba untuk menarik kesimpulan text sederhana atau kunci.
- Pemaksaan
  - Mencoba setiap kemungkinan kunci sehingga text sederhana dicapai

Algorithms

- Kepingan blok
  - —Proses text sederhana dalam ukuran blok yang tetap menghasilkan kepingan dari text yang ukurannya sama.
  - —Standar enkripsi data (DES)
  - —Triple DES (TDES)
  - —Standar enkripsi sebelumnya.

Standar data enkripsi

- Standar US
- 64 bit text blok datar
- 56 bit kunci
- dipecahkan di tahun 1998 oleh Electronic Frontier Foundation
  - Mesin khusus tujuan
  - Kurang dari tiga hari
  - DES sekarang tidak digunakan

Triple DEA

- ANSI X9.17 (1985)
- Diresmikan dlm standar DEA th 1999
- mengunakan 3 kunci dan 3 esekusi dari algoritma DEA
- Panjang kunci yang efektif 112 atau 168 bit
- Pelan
- Ukuran blok (64 bit) sangat kecil

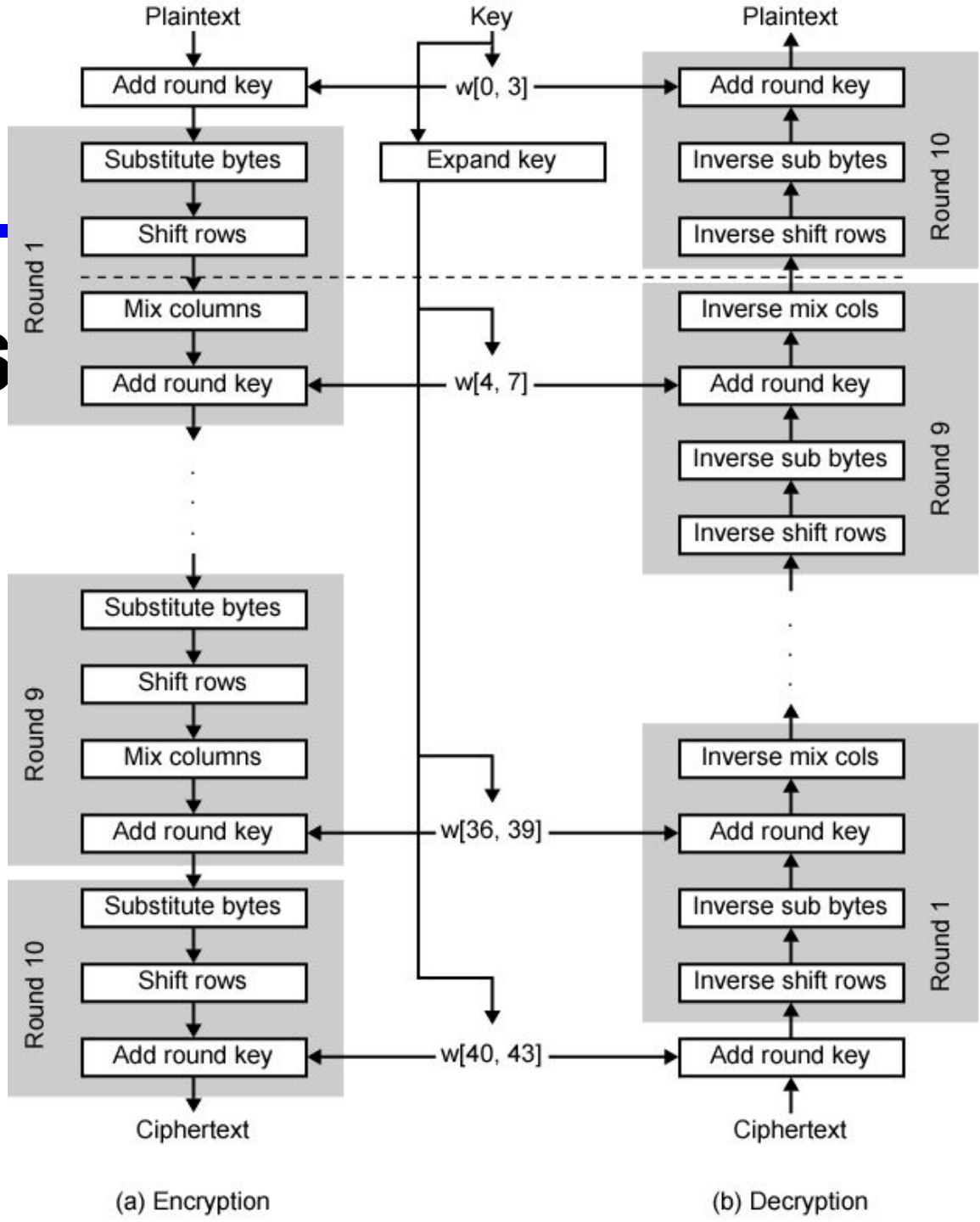
Standar enkripsi sebelumnya

- Institut standar dan teknologi nasional/National Institute of Standards and Technology (NIST) dalam 1997 disebut Advanced Encryption Standard (AES)
  - Kekuatan keamanan lebih besar sama dengan 3DES
  - Efesiensi mutu
  - Sandi rahasia simetris blok
  - Panjang blok 128 bits
  - Panjang kuncinya 128, 192, and 256 bits
  - Evaluasi memasukkan keamanan, efisiensi komputional,keperluan memory, kecocokan dan fleksibelitas hardware dan software
  - 2001, AES terbitan sebagai standar proses informasi federal (FIPS 197)

Deskripsi AES

- Mengambil kunci sepanjang 128 bit
- Input adalah single 128-bit blok
  - Menggambarkan sebagai matrik kotak
  - Blokn dikopi didalam array yang ditetapkan
    - dimodifikasi disetiap tingkatan
  - Setelah tingkatan terakhir, keadaan tersebut dikopi ke output matrix
- 128-bit kunci digambarkan sebagai kotak matrix dari byte
  - dikembangkan didalam array mengatur kata dari kunci
  - Setiap 4 byte
  - Mengatur 44 kata total kunci dari 128 bit
- Pemesanan byte oleh kolom
  - Pertama empat byte dari 128 bit input text sederhana four bytes of 128-bit plaintext input menempati kolom pertama dimatrix
  - Pertama empat byte dikembangkan kuncyu yang menempati kolom pertama dari w-matrix.

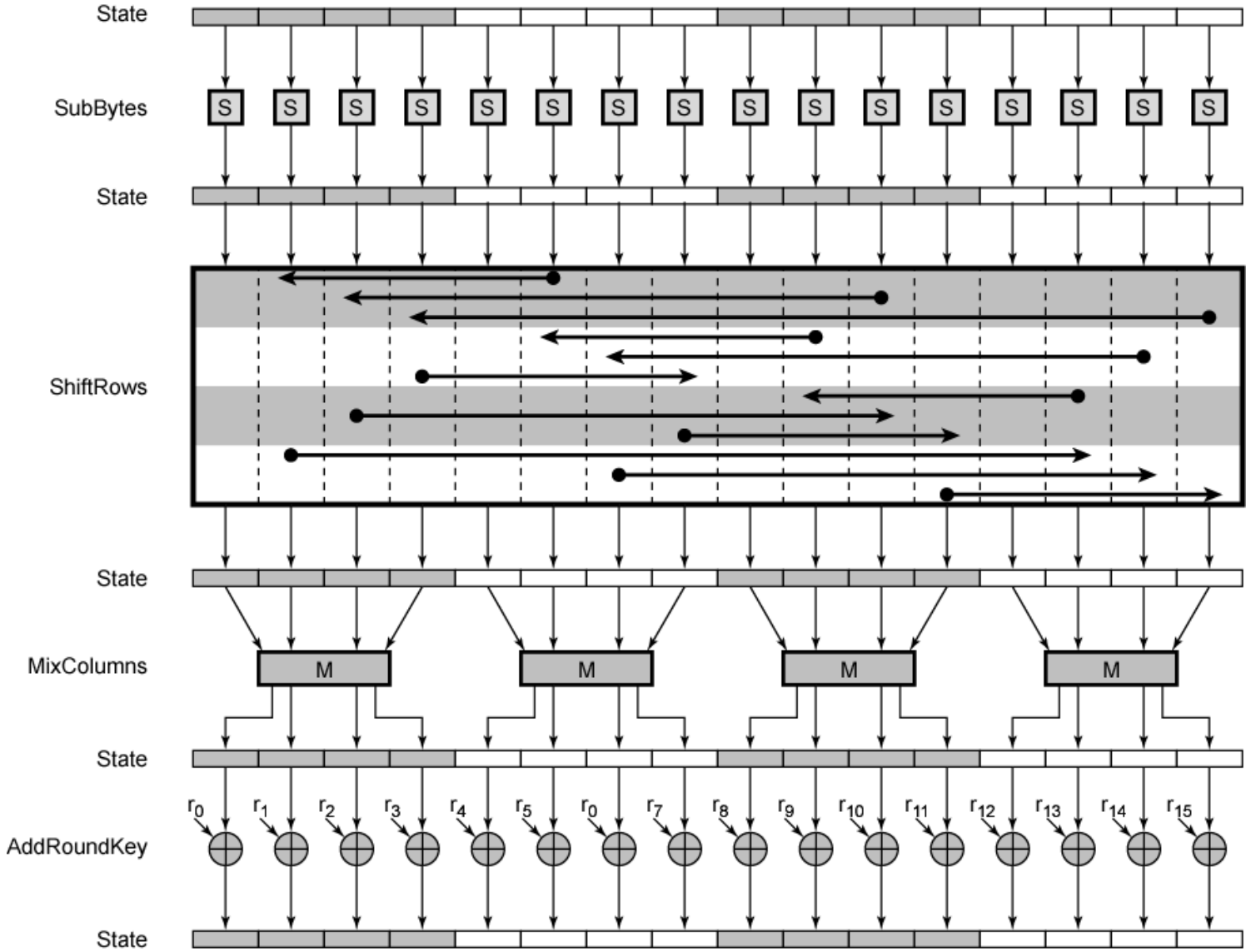
Enkripsi dan Dekripsi AES



Ulasan AES (1)

- Kunci dikembangkan didalam array dari empat puluh dua 32 bit kata,w[i]
  - Empat kata jelas (128 bit) menjalankan sebagai deretan kunci dari setiap deretan array
- Empaty tingkat perbedaan
  - Satu permutasi dan tiga subtitusi
    - Substitusi byte menggunakan tabel S-bax byte untuk melakukan subtitusi byte-byte dari blik.
    - Penggeseran baris merupakan permutasi yang dlakukan baris oleh baris
    - Kolom Campuran merupakan subtitusi yang merubah setiap byte dalam kolom sebagai fungsi dari semua dari byte dikolom
    - Menambah rentetan kunci XOR bitwise dari edaran blok dengan porsi dari pengembangan kunci
- Struktuir sederhana
  - Untuk kedua enkripsi dan dekripsi, both encryption and decryption, kepingan memulai menambah deretan stage kuncid
  - Diikuti oleh 9 deretan,
    - Setiap memasukkan semua 4 tingkatan
  - Diikuti oleh persepuluh tingkatan dari tiga tingkatan

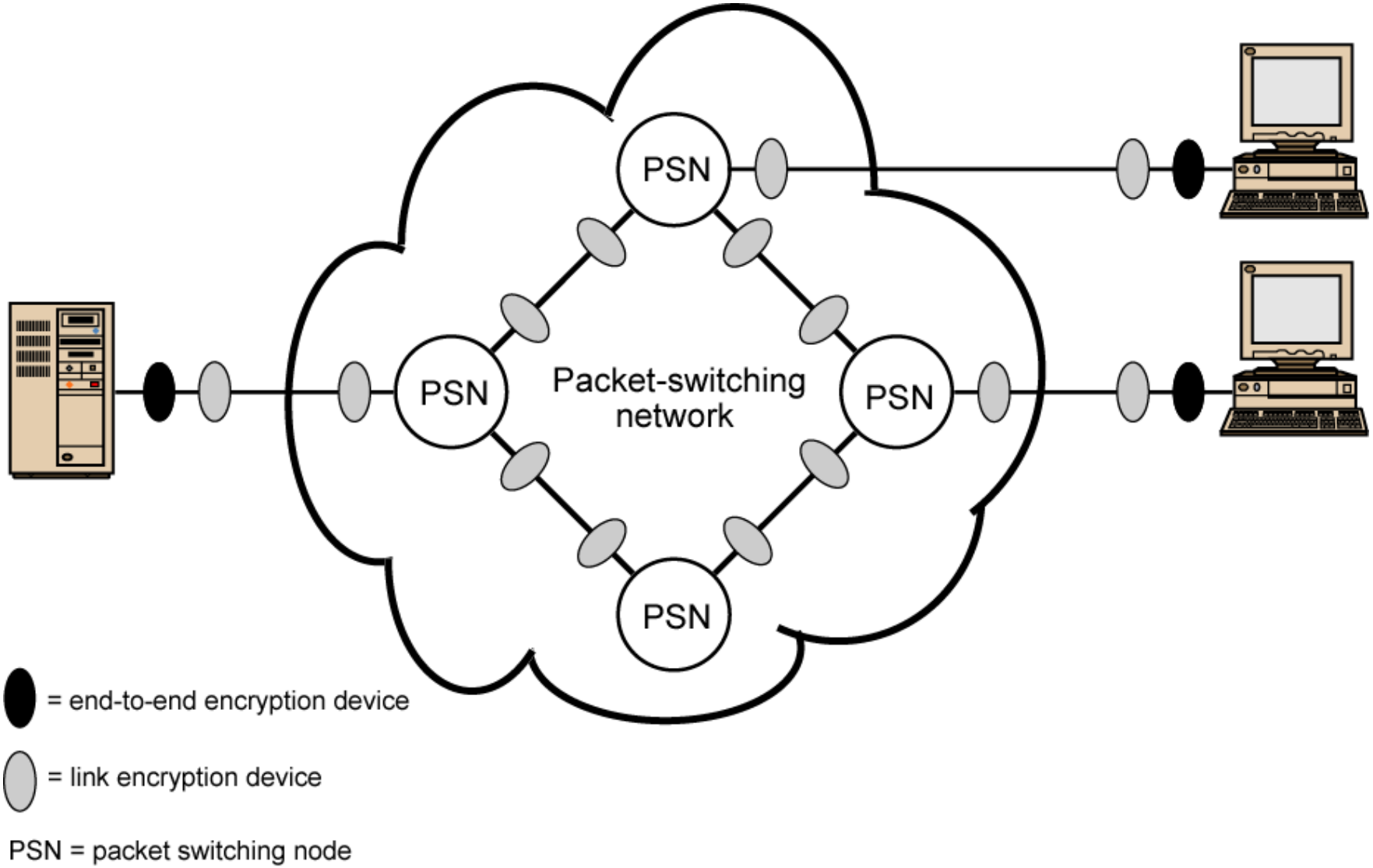
Deretan enkripsi AES



Ulasan AES (2)

- Hanya menambah deretan tingkatan kunci menggunakan kunci
  - Dengan menambah deretan tingkatan kunci diawal dan akhir
  - Beberapa tingkatan yang lain awal dan akhir,dibalik tanpa kunci
    - Bertambah tidak aman
- Menambah deretan tingkatan kunci tidak berat dengan sendirinya
  - 3 deretan lainnya berebut bit
  - mereka sendiri tidak menyediakan keamanan karena bukan kunci
- Setiap deretan memutarbalik dengan mudah
- Dekripsi menggunakan perkembangan kunci dalam perintah untuk memutar balik
  - Tidak identik algoritma enkripsi
- Mudah memeriksa bahwa enkripsi menemukan kembali plaintext
- Tingkat terakhir dari enkripsi dan diskripsi diantara 3 tingkatan
  - Untuk membuat kepingan kebalikkan

Lokasi Peralatan dari enkripsi



Hubungan enkripsi

- Masing-masing hubungan komunikasi equipped at both ends
- Keamanan semua trafik
- Tingkat keamanan tinggi
- Banyak persyaratan dari peralatan enkripsi
- Pesan harus dienkripsi di masing–masing switch untuk membaca alamat (virtual circuit number)
- Security vulnerable at switches
  - Particularly on public switched network

Enkripsi End to End

- Enkripsi dilakukan diakhir dari sistem
- Data dalam bentuk enkripsi yang melewati jaringan unaltered
- Tujuan membagi kunci dengan sumber untuk decrypt
- Host hanya dapat enkripsi data user
  - Jadi node switching tidak dapat membaca header atau paket routing
- Pola lalu lintas tidak aman

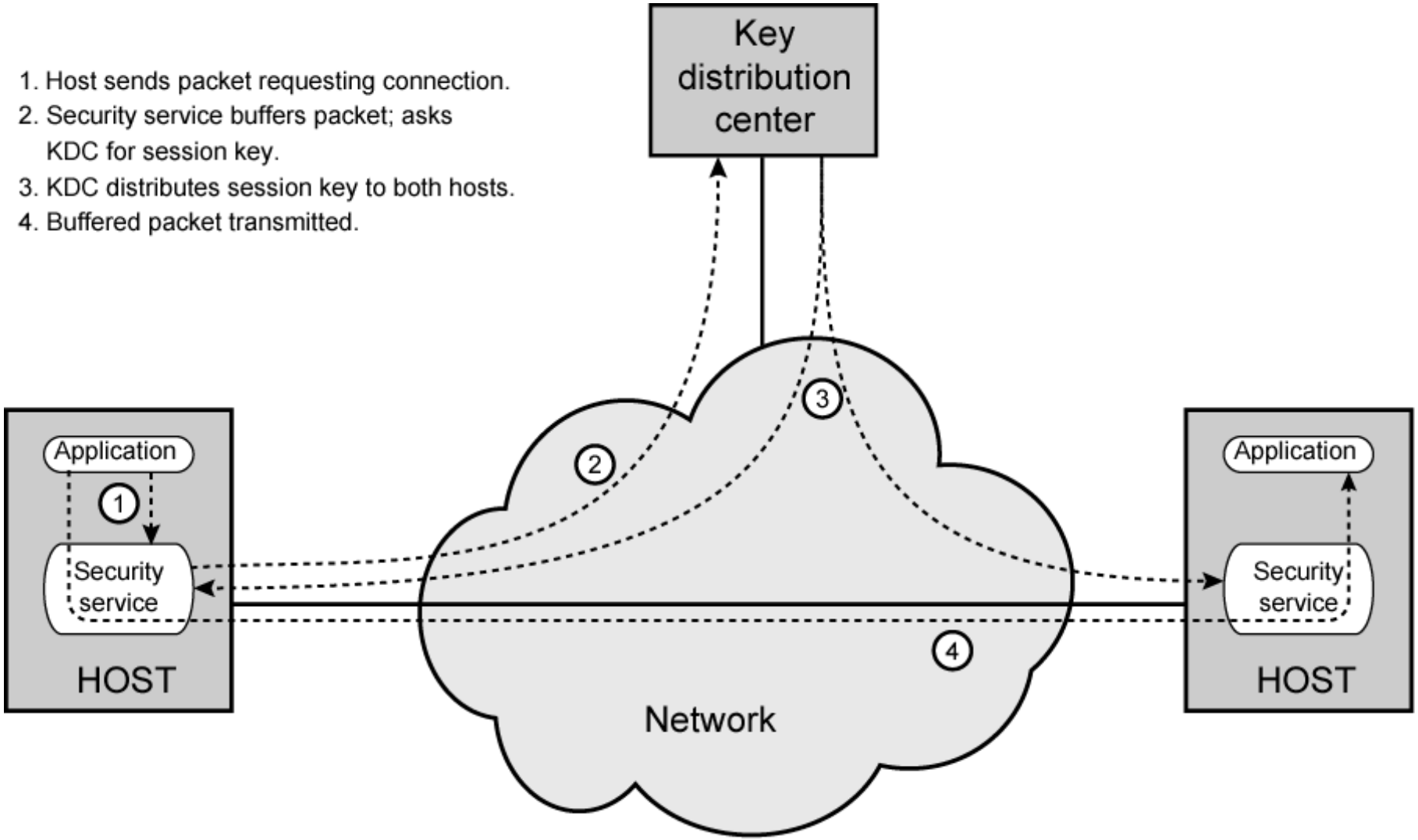
- Menggunakan sambungan end to end

Distribusi Key

- Kunci diseleksi A dan dikirim ke B
- Three party memilih key dan mengirimkan ke A dan B
- Menggunakan old key untuk enkripsi dan transmisi new key dari A dan B
- Menggunakan old key untuk transmisi kunci baru dari third party ke A dan B

Distribusi key otomatik (diag)

1. Host sends packet requesting connection.
2. Security service buffers packet; asks KDC for session key.
3. KDC distributes session key to both hosts.
4. Buffered packet transmitted.



Distribusi key otomatik

- Session Key
  - Digunakan untuk durasi dari satu logical connection
  - Merusak pada akhir session
  - Digunakan untuk pemakai data
- Permanent key
  - Digunakan untuk distribusi keys
- Pusat distribusi key
  - Determinasi system yang boleh komunikasi
  - Menyediakan key satu sesi untuk koneksi
- Security service module (SSM)
  - Mennjukkan enkripsi end to end
  - Mengandung keys untuk host

Traffic Padding

- Menghasilkan potongat text yang berkesinambungan
- Jika tidak ada text datar untuk encoding, maka akan mengirim data acak
- Membuat ketidakmungkian analisa traffic

Autentikfikasi pesan

- Protection against active attacks
  - Pemalsuan data
  - Eavesdropping
- Pesan adalah authentic jika datang dari source yang diminta
- Pengesahan mengijinkan receiver untuk mengklasivfikasi bahwa pesan itu asli atau authentic
  - Message belum diubah
  - Message dari sumber yang asli
  - Message timeline

Authentication Using Encryption

- Mengasumsikan penerima dan pengirim yang hanya mengetahui kunci
- Message meliputi:
  - —error detection code
  - —sequence number
  - —time stamp

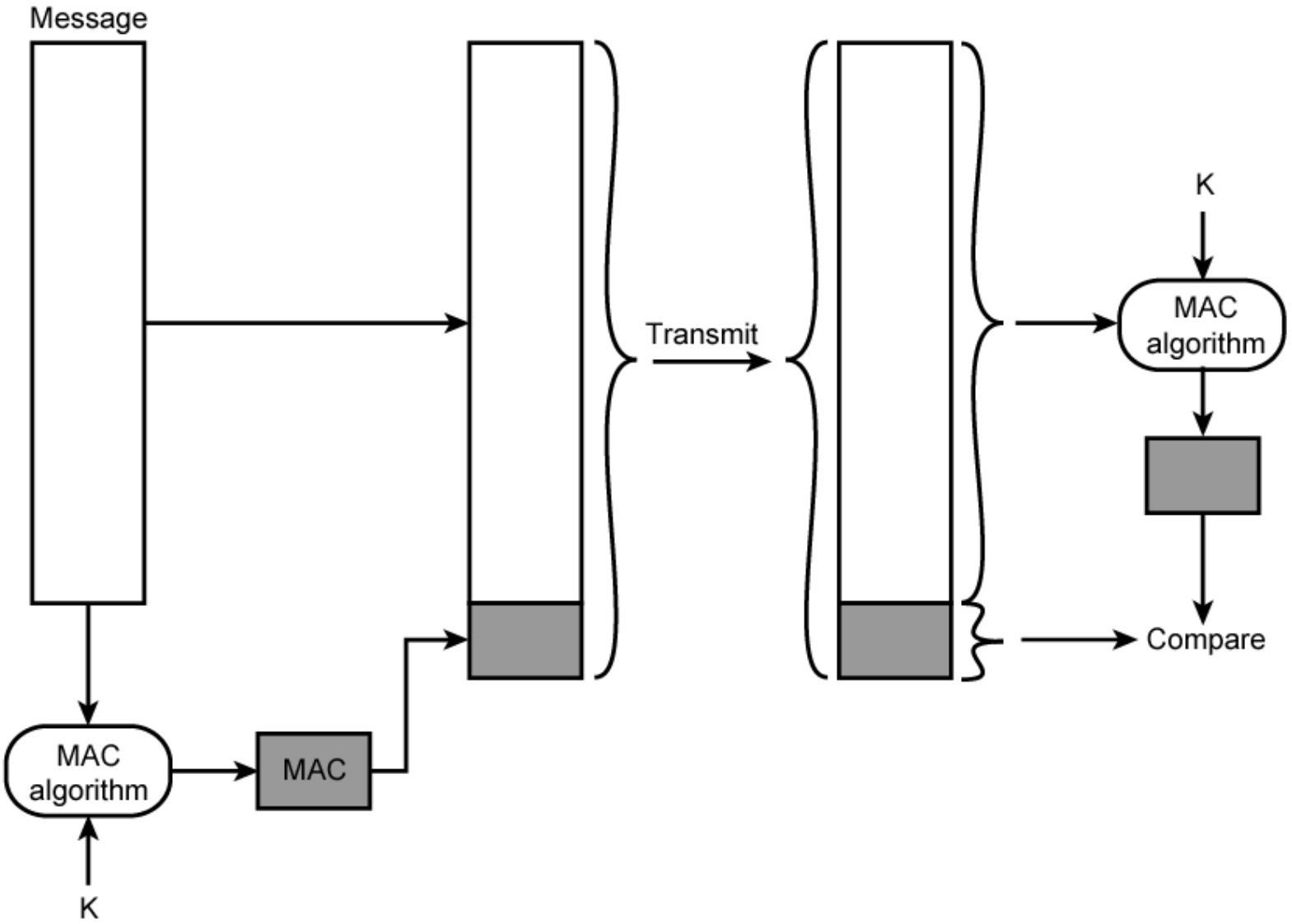
Authentication Without Encryption

- Authentication tag generated and appended to each message
- Message not encrypted
- Berfungsi untuk:
  - —Messages broadcast ke multiple destinations
    - Have one destination responsible for authentication
  - —One side heavily loaded
    - Encryption adds to workload
    - Can authenticate random messages
  - —Programs authenticated tanpa encryption bisa dieksekusi tanpa decoding

Message Authentication Code

- Generate authentication code based on shared key and message
- Common key shared between A and B
- Jika hanya pengirim dan penerima yang mengetahui key dan code yang sesuai:
  - Receiver assured message has not altered
  - Receiver assured message is from alleged sender
  - If message has sequence number, receiver assured of proper sequence

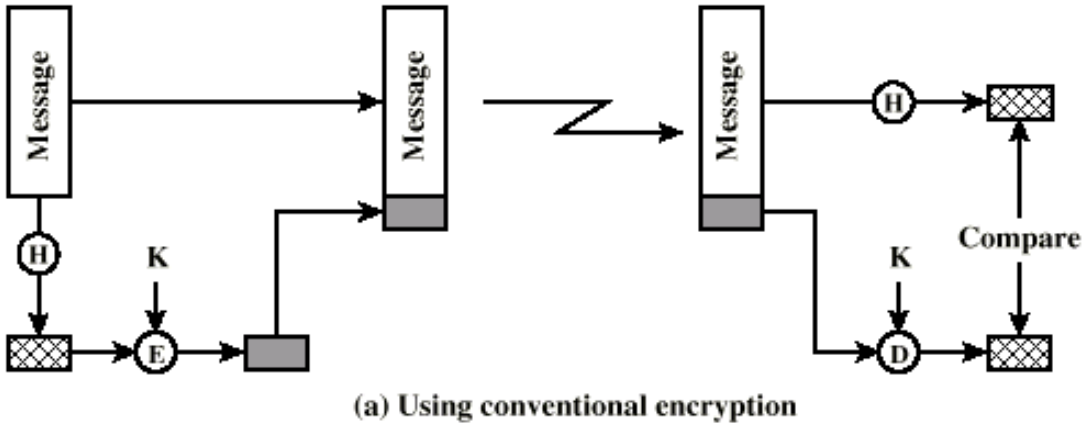
Message Authentication Using Message Authentication Code



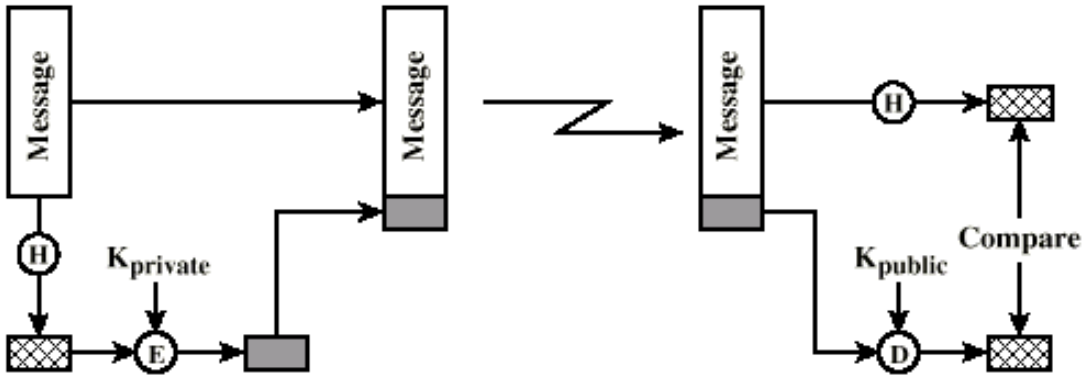
One Way Hash Function

- Accepts variable size message and produces fixed size tag (message digest)
- Keuntungan pengesahan tanpa encryption
  - —Encryption lambat
  - —Encryption hardware mahal
  - —Encryption hardware optimized to large data
  - —Algorithms covered by patents
  - —Algorithms subject to export controls (from USA)

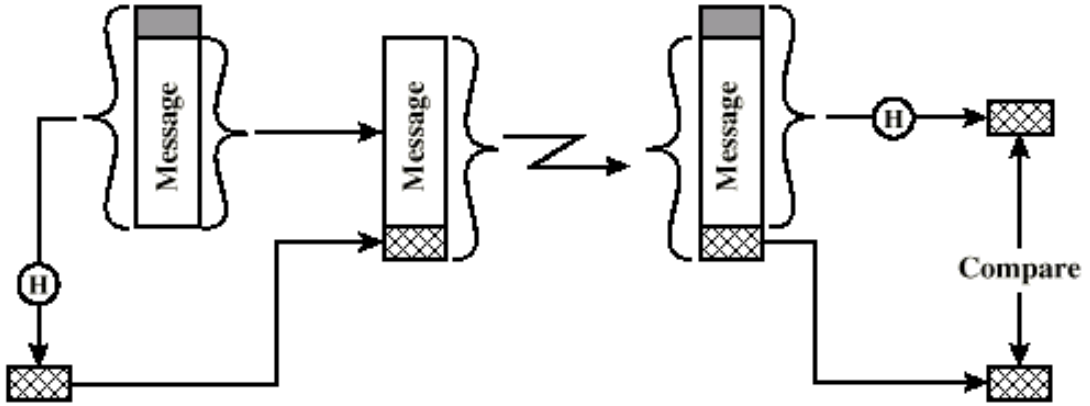
Using One Way Hash



(a) Using conventional encryption



(b) Using public-key encryption



(c) Using secret value

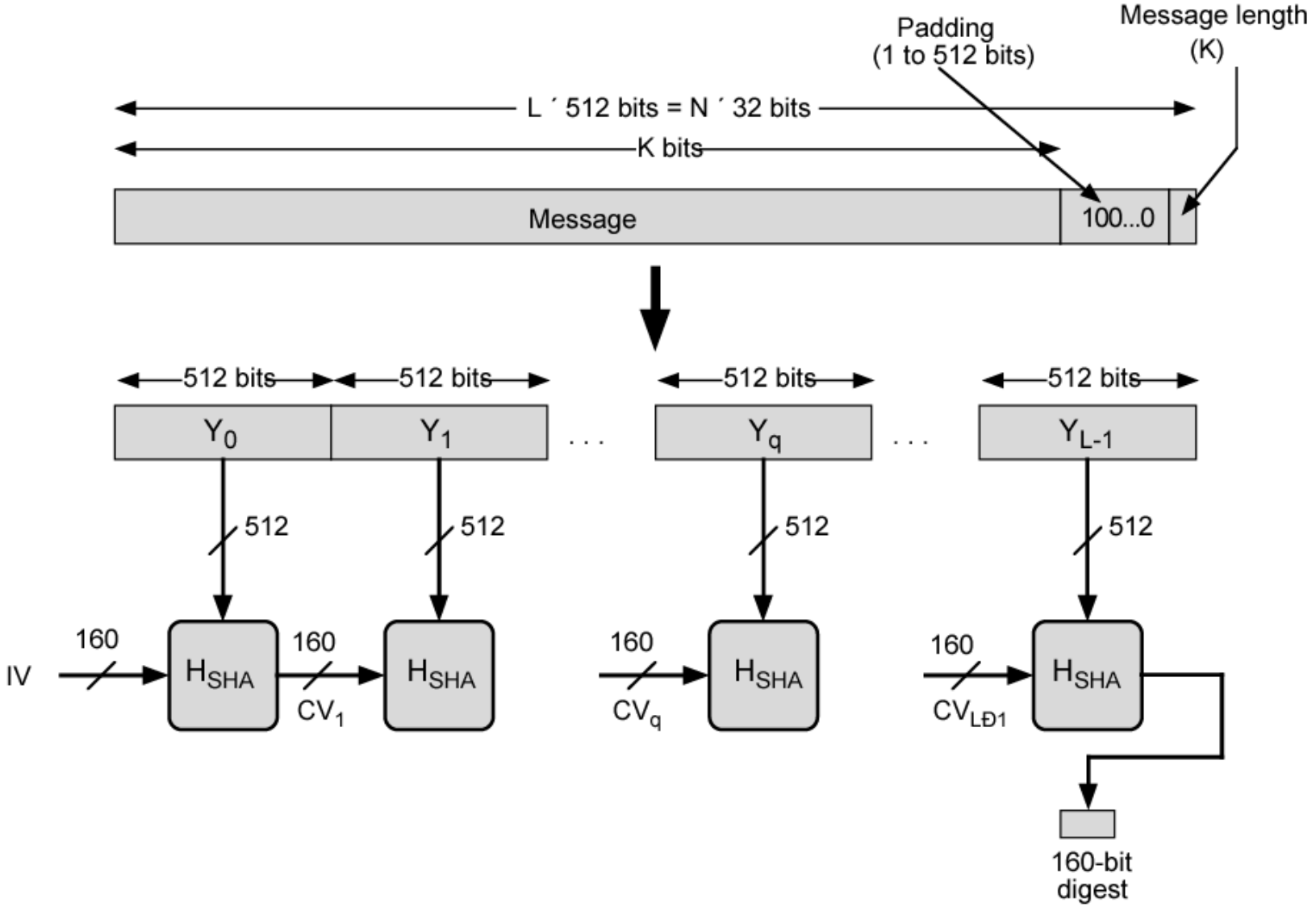
Secure Hash Functions

- Hash function must have following properties:
  - Can be applied to any size data block
  - Produce fixed length output
  - Mudah untuk menghitung
  - Not feasible to reverse
  - Not feasible to find two message that give the same hash

SHA-1

- Secure Hash Algorithm 1
- Pesan masukan lebih kecil dari 2^{64} bits
  - Diproses di 512 bit blocks
- Keluaran 160 bit digest

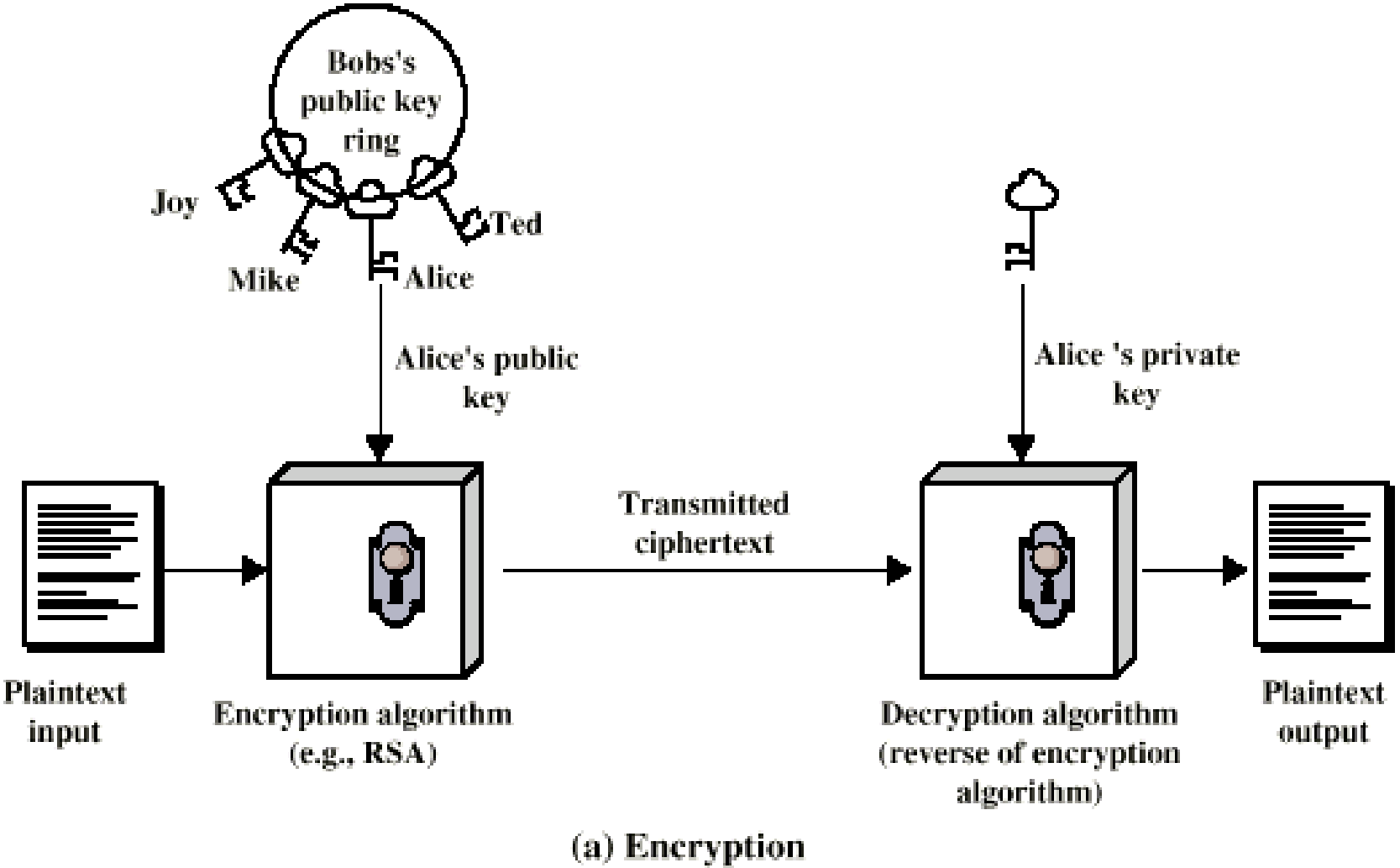
Message Digest Generation Using SHA-1



Public Key Encryption

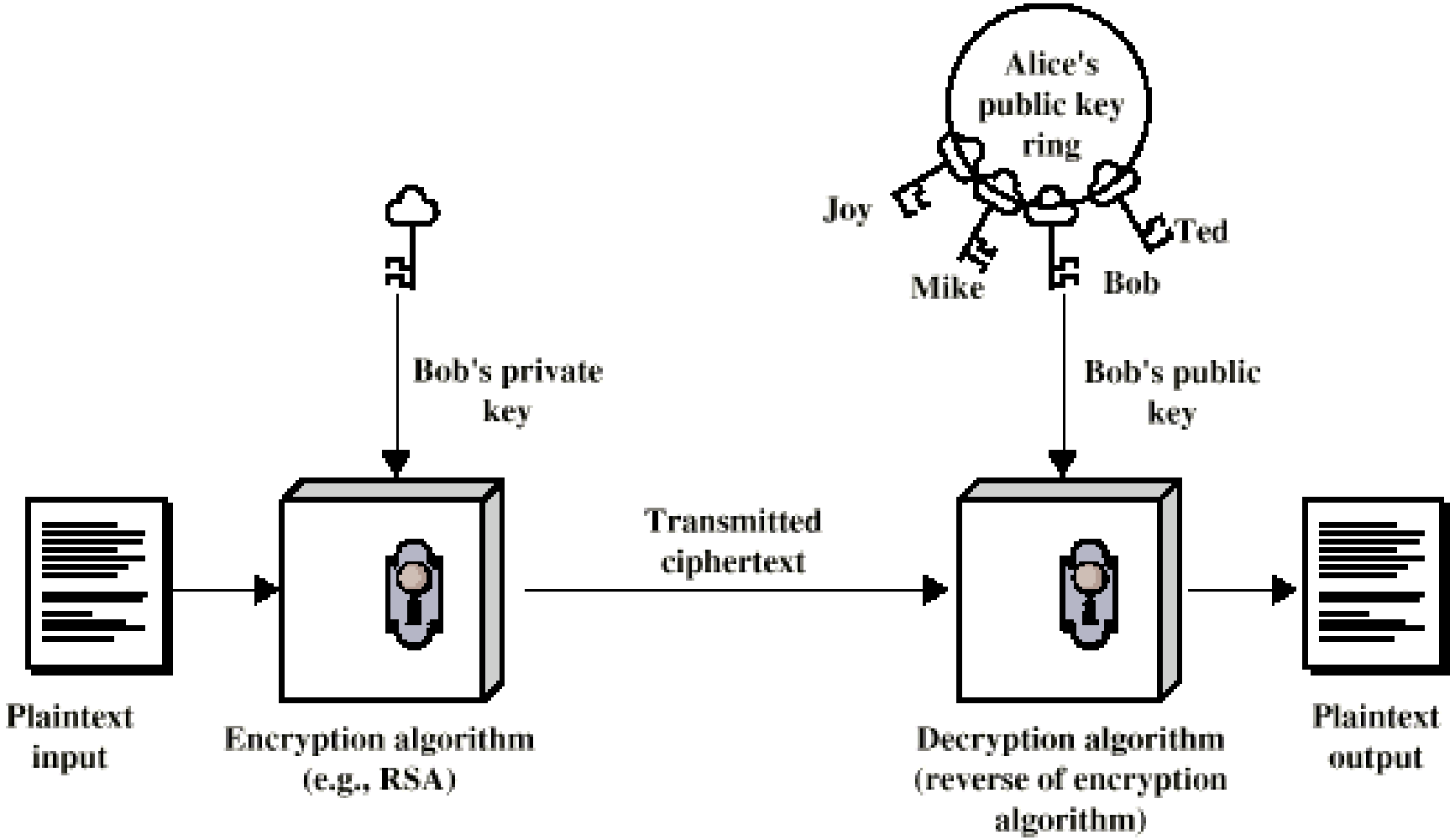
- Dibangun di mathematical algorithms
- Asymmetric
  - Menggunakan dua separate keys
- Ingredients
  - Plain text
  - Encripsi algoritma
  - Public dan private key
  - Cipher text
  - Deskripsi algoritma

Public Key Encryption - Encryption



(a) Encryption

Public Key Encryption – Authentication



(b) Authentication

Public Key Encryption - Operation

- One key made public
  - —Digunakan untuk encryption
- Other kept private
  - —Digunakan untuk decryption
- Infeasible to determine decryption key given encryption key and algorithm
- Either key can be used for encryption, the other for decryption

Steps

- User generates pair of keys
- User places one key in public domain
- To send a message to user, encrypt using public key
- User decrypts menggunakan private key

Digital Signature

- Sender encrypts message with their private key
- Receiver can decrypt using senders public key
- This authenticates sender, who is only person who has the matching key
- Does not give privacy of data
  - Decrypt key is public

RSA Algorithm

Key Generation

Select p, q	p and q both prime
Calculate $n = p \times q$	
Calculate $\phi(n) = (p-1)(q-1)$	
Select integer e	$\gcd(\phi(n), e) = 1;\ 1 < e < \phi(n)$
Calculate d	$d = e^{-1} \bmod \phi(n)$
Public key	$KU = \{e, n\}$
Private key	$KR = \{d, n\}$

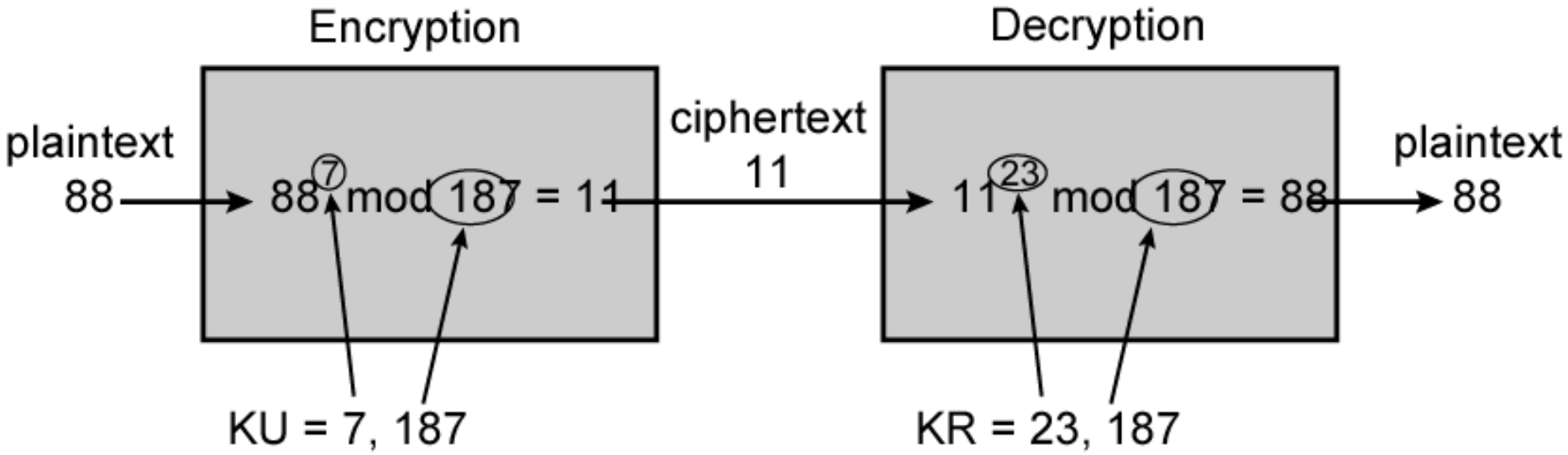
Encryption

Plaintext:	$M < n$
Ciphertext:	$C = M^e \pmod{n}$

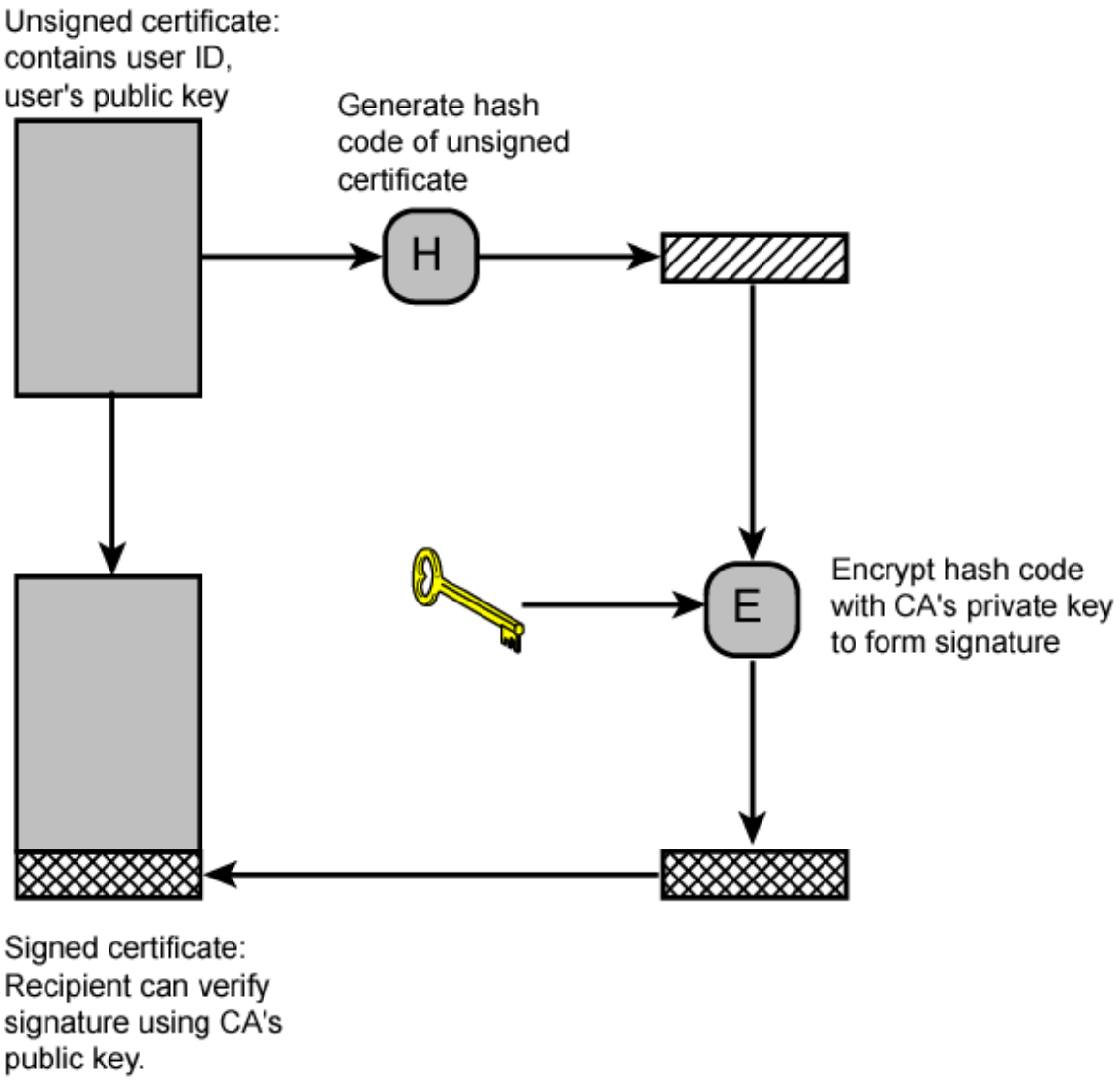
Decryption

Ciphertext:	C
Plaintext:	$M = C^d \pmod{n}$

RSA Example


Encryption
Decryption
plaintext
88
88^7 mod 187 = 11
ciphertext
11
11^23 mod 187 = 88
plaintext
88
KU = 7, 187
KR = 23, 187

Public Key Certificate Use



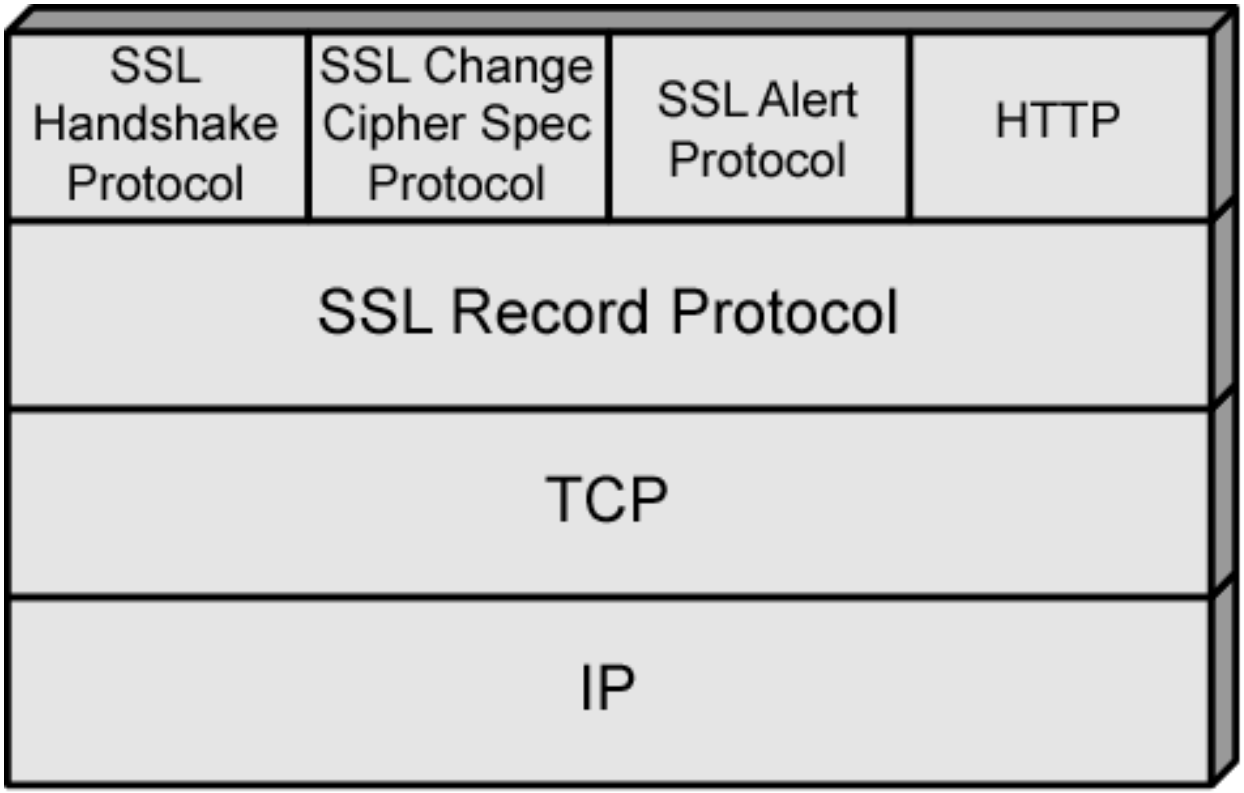
Secure Sockets Layer
Transport Layer Security

- Service keamanan
- Transport Layer Security didefinisi di RFC 2246
- SSL general-purpose service
  - —Set of protocols that rely on TCP
- Two implementation options
  - —Part of underlying protocol suite
    - Transparent to applications
  - —Embedded in specific packages
    - E.g. Netscape and Microsoft Explorer and most Web servers
- Minor differences between SSLv3 and TLS

SSL Architecture

- SSL menggunakan TCP untuk menyediakan keandalan end-to-end service keamanan
- SSL two layers of protocols
- Record Protocol provides basic security services to various higher-layer protocols
  - In particular, HTTP can operate on top of SSL
- Three higher-layer protocols
  - Handshake Protocol
  - Change Cipher Spec Protocol
  - Alert Protocol
  - Used in management of SSL exchanges (see later)

SSL Protocol Stack



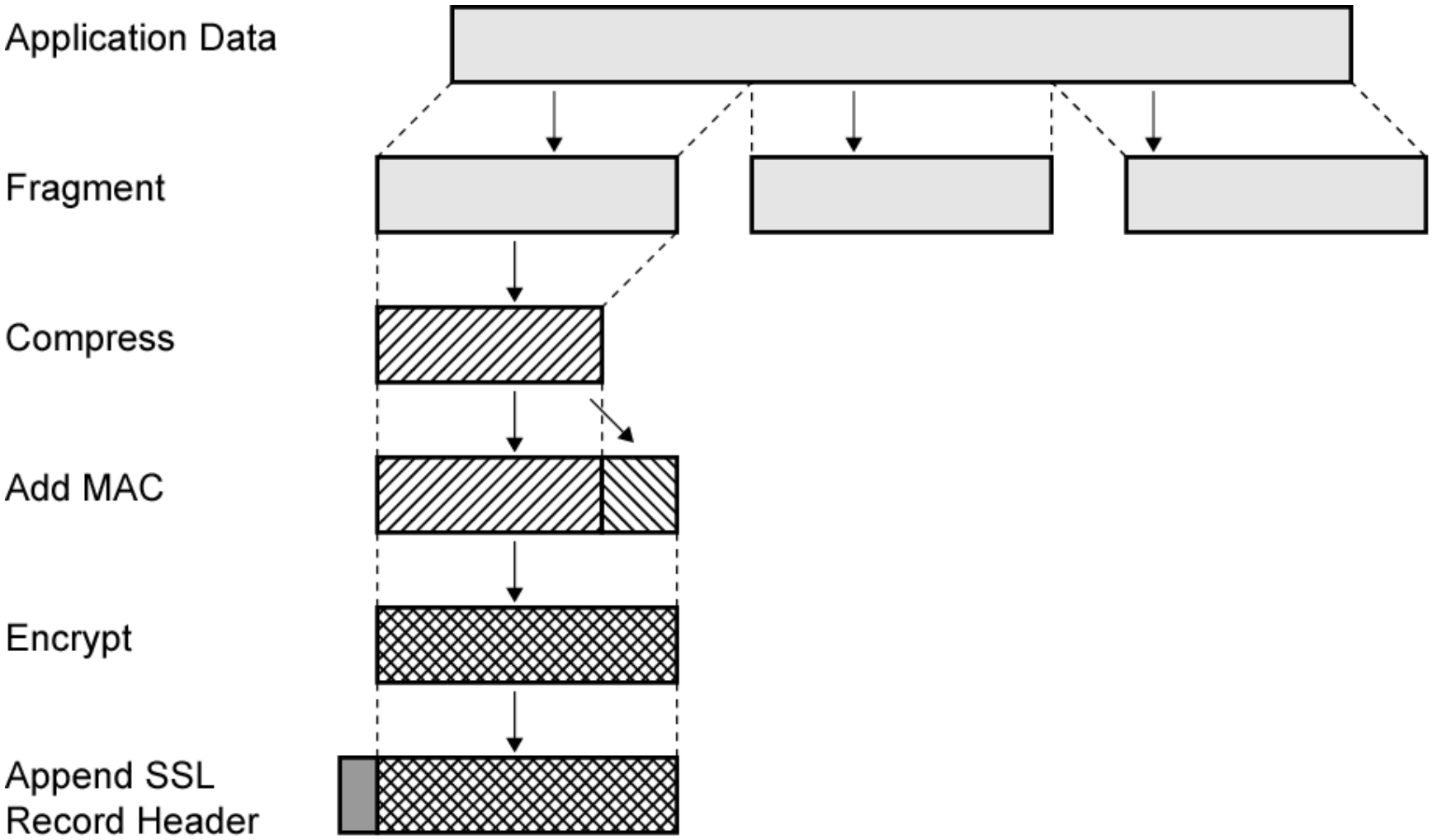
SSL Connection and Session

- Connection
  - Transport that provides suitable type of service
  - Peer-to-peer
  - Transient
  - Every connection associated with one session
- Session
  - Association antara client dan server
  - Dibuat oleh Handshake Protocol
  - Define set of cryptographic security parameters
  - Used to avoid negotiation of new security parameters for each connection
- Maybe multiple secure connections between parties
- May be multiple simultaneous sessions between parties
  - Not used in practice

SSL Record Protocol

- Confidentiality
  - Handshake Protocol defines shared secret key
  - Digunakan untuk symmetric encryption
- Message Integrity
  - Handshake Protocol defines shared secret key
  - Digunakan untuk membentuk message authentication code (MAC)
- Each upper-layer message fragmented
  - 2^{14} bytes (16384 bytes) or less
- Compression optionally applied
- Compute message authentication code
- Compressed message plus MAC encrypted using symmetric encryption
- Prepend header

SSL Record Protocol Operation



Record Protocol Header

- Content Type (8 bits)
  - change_cipher_spec, alert, handshake, and application_data
  - No distinction between applications (e.g., HTTP)
    - Content of application data opaque to SSL
- Major Version (8 bits) – SSL v3 is 3
- Minor Version (8 bits) - SSLv3 value is 0
- Compressed Length (16 bits)
  - Maximum 2^{14} + 2048
- Record Protocol then transmits unit in TCP segment
- Menerima data decrypted, verified, decompressed, dan reassembled dan kemudian dikirim

Change Cipher Spec Protocol

- Menggunakan Record Protocol
- Satu pesan
  - —Satu byte bernilai 1
- Cause pending state to be copied into current state
  - —Updates cipher suite to be used on this connection

Alert Protocol

- Convey SSL-related alerts to peer entity
- Alert messages compressed and encrypted
- Dua byte
  - —Byte pertama warning(1) atau fatal(2)
    - Jika fatal, SSL dengan seketika mengakhiri koneksi
    - Other connections on session may continue
    - No new connections on session
  - —Byte kedua mengindikasi specific alert
  - —E.g. fatal alert is an incorrect MAC
  - —E.g. nonfatal alert is close_notify message

Handshake Protocol

- autentifikasi
- Negotiate encryption and MAC algorithm and cryptographic keys
- Digunakan sebelum semua aplikasi data dikirim

Handshake Protocol – Phase 1 Initiate Connection

- versi
  - Versi tertinggi SSL dimengerti oleh client
- acak
  - Client-menghasilkan structure yang acak
  - 32-bit timestamp and 28 bytes from secure random number generator
  - digunakan selama mengganti key untuk mencegah replay attacks
- Session ID
  - Panjang variable
  - Nonzero indicates client wishes to update existing connection or create new connection on session
  - Zero indicates client wishes to establish new connection on new session
- CipherSuite
  - List of cryptographic algorithms supported by client
  - Each element defines key exchange algorithm and CipherSpec
- Compression Method
  - Compression methods client supports

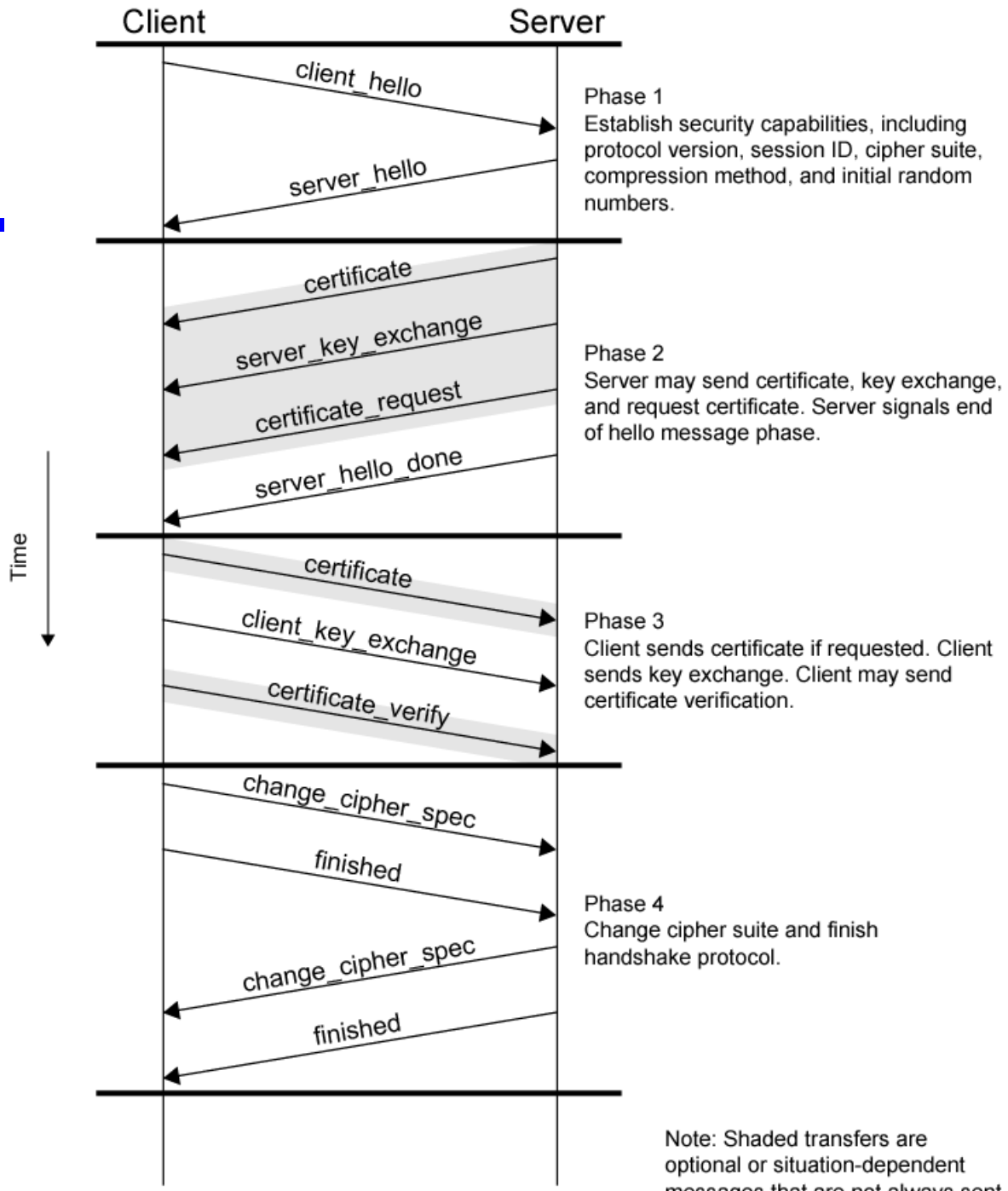
Handshake Protocol – Phase 2, 3

- Client menunggu selama server mengirimkan pesan helo
  - Prameter sama sebagai client helo
- fase 2 tergantung skema enkripsi yang pokok
- Pesan terakhir dalam fase 2 server_done
  - Diperlukan
- 3 fase
  - Siap menerima dari server_done, client memeriksa sertifikat jika diperlukan dan mengecek parameter server_helo
  - Client mengirimkan pesan ke server,tergantung kunci skema pokok umum

Handshake Protocol – Phase 4

- Pengaturan komplit
- Client mengirimkan pertukaran spesifikasi
- Menunggu salinan CipherSpec dalam pengukur CipherSpec
  - Bagian Handshake Protocol tidak dipertimbangkan
  - Mengirim dengan menggunakan pertukaran protokol Cipher Spec
- Client mengirimkan pesan yang terakhir dibawah algoritma baru, kunci dan rahasia
- Pesan yang terakhir memeriksa pertukaran kunci dan keautentikkan
- Server mengirimkan pertukaran CipherSpec-nya
- Menunggu Transfer pengukur CipherSpec
- Mengirimkan pesan terakhirnya
- Handshake komplit

Handshake Protocol Action



IPv4 and IPv6 security

- IPSec
- Mengamankan kantor cabang mengkoneksi di internet
- Mengamankan jalan masuk di internet
- Konektifitas Extranet and intranet
- Mempertinggi perdagangan keamanan elektronik

Keleluasaan IPSec

- autentikasi header
- Peralatan keamanan Dienkapsul
- Pertukaran kunci
- RFC 2401,2402,2406,2408

Assosiasi keamanan

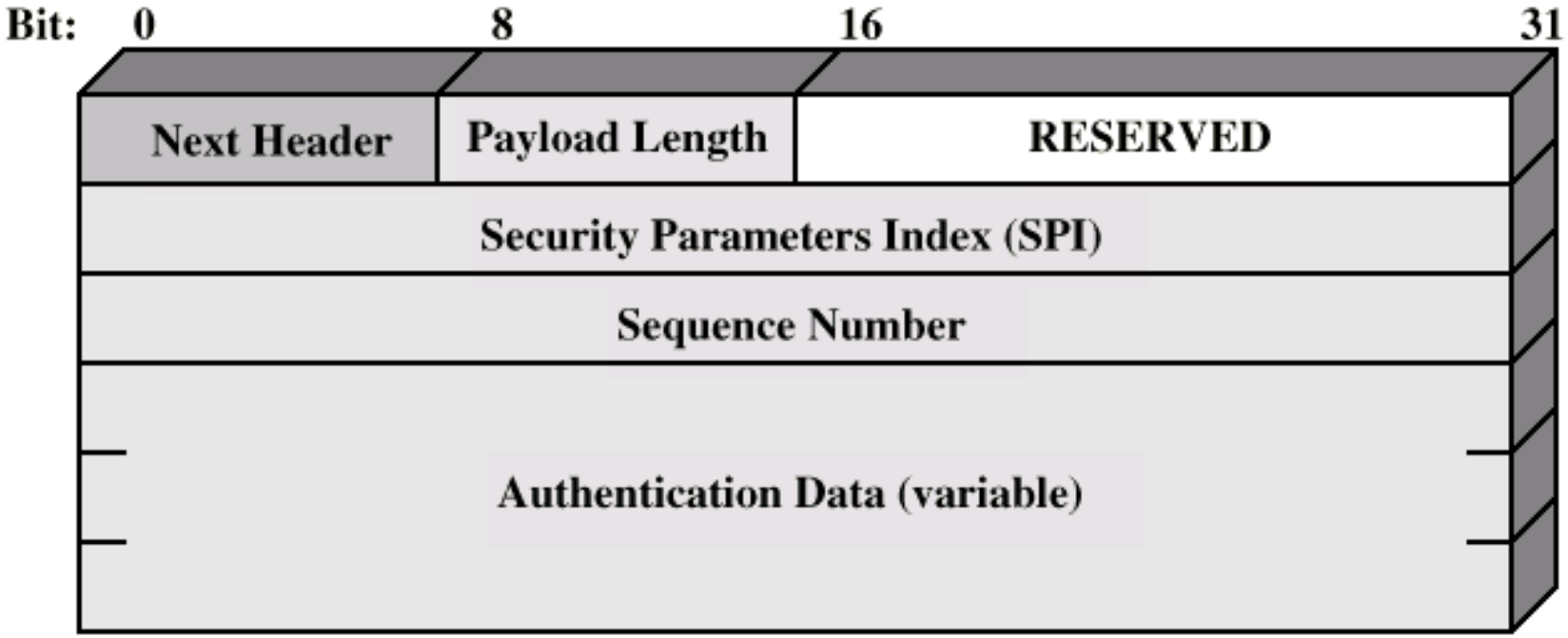
- Satu jalan menghubungkan antara pengirim dan penerima
- selama 2 jalan ,2 assosiasi dibutuhkan
- Parameter identifikasi 3 SA
  - Index parameter keamanan
  - Alamat tujuan IP
  - Pengidentifikasi keamanan protokol

Parameter SA

- Urutan penghitug nomor
- Urutan penghitung luapan
- Anti-jawaban windows
- Informasi AH
- Informasi ESP
- Seumur hidup
- IPSec protocol mode

  Tembusan, pengangkutan atau wildcard
- Jalur kecil MTU

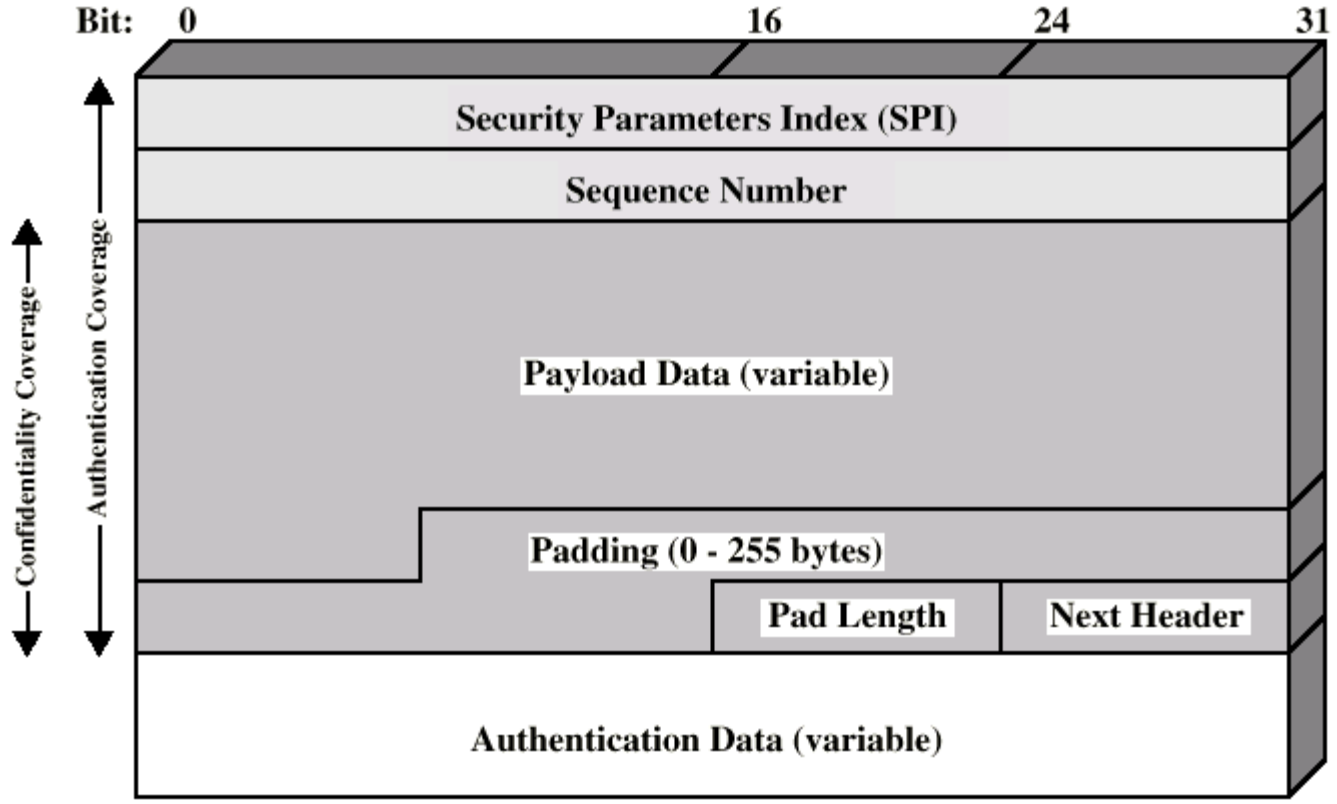
Autentik Header



Encapsulating Security Payload

- ESP
- Pelayanan dapat dipercaya

Paket ESP


Bit:
0
16
24
31
Security Parameters Index (SPI)
Sequence Number
Payload Data (variable)
Padding (0 - 255 bytes)
Pad Length
Next Header
Authentication Data (variable)
Confidentiality Coverage
Authentication Coverage

Required Reading

- Stallings bab 21
- Web sites di public/private key encryption
- RFCs mentioned
  - www.rfc-editor.org