Kapitel 12 Netzsicherheit

12. NETZSICHERHEIT

Vorbem : In Anbetracht der zeitlichen Restriktionen nur rudimentäre Behandlung dieses wichtigen Themas möglich
→ weitere Details, vgl. einschlägige Vertiefungs-/Wahlgebietsvorlesungen des AB SVS

12.1 Allgemeines zu Datenschutz und Datensicherung in verteilten Systemen und Rechnernetzen

Datenschutz : Schutz identifizierbarer Daten über persönliche und sachliche Verhältnisse von Personen.

Datensicherung : Schutz von Daten vor
- Zerstörung
- Verfälschung
- Wertverlust

entstehend durch:
- gerätetechnische Fehlfunktionen
- (un)beabsichtigte Handlungen von Personen.

Zum Begriff „Datensicherung“ :

a) **Datensicherung** (im **engeren** Sinne) :
vgl. hierzu auch Datensicherungsschicht
(gemäß OSI-Architekturmodell)
→ dort insbesondere Schutz von Daten vor Verfälschung bei Transport zwischen direkt miteinander (durch gemeins. Übertragungsmedium) verbundenen Knoten.

b) **Datensicherung** (im **weiteren** Sinne) :
vgl. obige Begriffsdefinition (auf voriger Folie)
→ in Kap. 12 : Verwendung des Datensicherungsbegriffes in seinem weiteren Sinne !

Schutzmaßnahmen in (verteiltem) DV-System :

- Abgangskontrolle (Datenverlust)
- Speicherkontrolle
- Benutzerkontrolle
- Zugriffskontrolle
- Transportkontrolle
  (vgl. Bundesdatenschutzgesetz)

Angriffsmöglichkeiten auf Daten während ihrer

- *Übertragung* → Leitung, Funkstrecke (Lauscher, Fälscher)

- *(Zwischen-)Speicherung*
  - in Vermittlungsrechnern
  - im Hauptspeicher von Hosts
  - auf Sekundärspeicher von Hosts

Gründe für Angriffe auf verteilte Systeme (VS) :

- leichte Zugriffsmöglichkeit auf (evtl. entfernt abgespeicherte) Datenobjekte und sonstige Betriebsmittel (BM) des VS

  → Datenmissbrauch, BM-Benutzung ohne Bezahlung, ...

- zunehmend mehr und wertvollere Information zwischen kommunizierenden Rechnern (Großrechnern, Workstations, PCs und Servern) ausgetauscht, z.B. Banken, Militär, Behörden, Industrie

  → unbefugter Zugriff auf diese Information

- neue Netztechnologien, die gewisse Arten von Angriffen erleichtern (z.B. offene Systeme, Kopplung von Rechnernetzen, Funknetze/drahtlose DÜ)

  → vgl. Sicherheitslücken in Windows, UNIX, Internet, GSM-Netze, WLANs, ...

Mögliche Eindringlinge in verteilten Systemen :

- „legitimer“ Benutzer (mit Fehlverhalten)
- Person ohne Befugnis für die Systembenutzung (bis hin zu Geheimdiensten, vgl. u.a. NSA-Abhörskandal im Jahr 2013)

Verletzung der Sicherheitsanforderungen eines VS durch :

- *unauthorisierte Nutzung und Verbreitung von Information*;
- *unauthorisierte Modifikation von Information*;
- *unauthorisierte Inanspruchnahme von Betriebsmitteln* (des Kommunikationssystems oder der Endsysteme);
- (gezieltes) *Stören des Netz-/Systembetriebs*.

➢ **Netzsicherheit** umfasst :

- Datensicherheit im Netz, sowie den
- Schutz gegen gewollte, unzulässige Einwirkungen auf das Netz und dessen Aufträge.

➢ **Anforderungen an Sicherheit**
(insbesondere bei Rechen- und Kommunikationssystemen) u.a.

- **Vertraulichkeit** :
  Objekte (Daten, Programme, u.ä.) nur von den dazu berechtigten Personen gelesen/benutzt (Gewährleistung eines hohen Maßes an Vertraulichkeit : auch **Geheimhaltung**).

- **Integrität** :
  Objekte befinden sich in rechtmäßigem Zustand, d.h. sie wurden nicht unbefugt verändert.

- **Verfügbarkeit** :
  Objekte können von den dazu berechtigten Personen ohne Einschränkung der jeweils geltenden Berechtigungen benutzt oder verändert werden.

- **Nichtabstreitbarkeit** :
  Eine Aktion, Nachricht oder ein Dokument kann eindeutig einer Person als Erzeuger (oder Empfänger) zugeordnet werden. Diese kann ihre Rolle nicht abstreiten; Sender und Empfänger können sich gegenseitig auf die Identität des anderen verlassen, da sie im Konfliktfall auch später noch bewiesen werden kann.

- **Authentizität** :
  Identität eines Benutzers oder Systems ist sichergestellt → kann nicht vorgetäuscht werden.

Erschwernisse für die Gewährleistung von Sicherheit in verteilten Systemen :

1) sehr große Anzahl möglicher Angreifer in Netzen; Datenobjekte evtl. weit entfernt von ihren Benutzern abgespeichert; Prozesse zur Bearbeitung von Benutzeraufträgen evtl. auf entfernten Rechnern ablaufend
   ⇒ ergo : ggf. große Datenmengen zwischen Knoten auszutauschen
   Probleme :
   - Kontrolle der Zugriffe auf Objekte
   - Identitätskontrolle für Benutzer, Prozesse, etc.

2) Netzkonfigurationen sehr dynamisch, u.a. Konfigurationsmodifikationen bei Ausfällen, Wiedereingliederung von Komponenten nach Reparatur/Beschaffung
   ⇒ Dynamik zu berücksichtigen durch Sicherheitsmechanismen

3) gekoppelte Rechnernetze häufig mit eigenem Netzmanagement
   ⇒ bei Kommunikation über Netzgrenzen : Grad an Sicherheit gegeben durch „schwächstes Glied in Kette“

4) bei wenig abhörsicheren Übertragungsmedien (Satellitenkommunikation, verdrillte Drähte, Rund-/Richtfunk, u.ä.): Abhören der übertragenen Signale und ihre Verfälschung möglich
   ⇒ Verschlüsselung der Daten vor Übertragung; evtl. Schlüsselverwaltung notwendig

5) Heterogenität der Protokolle und Architekturen von Netzen
   ⇒ Integration von Sicherheitsmechanismen verkompliziert sich

nota bene : generelle Schwierigkeit durch Gegensatz
- ***Offenheit*** von Systemen ⇒ ***Freizügigkeit*** bei Kommunikation
- ***Schutzbedürfnisse*** ⇒ ***Restriktionen*** bei Kommunikation

Bedrohungsarten für die Interprozesskommunikation in Netzen

- **Passive Angriffe** :
  passive Beobachtung des Nachrichtenflusses, ohne ihn zu modifizieren

  - **Ermittlung der Nachrichteninhalte**
    durch Abhören von Verbindungen
    → nicht-authorisierte Nutzung oder Verbreitung von (geheimer oder vertraulicher) Information

  - **Verkehrs(fluss)analyse**
    → Feststellen bestehender Kommunikationsbeziehungen und -intensitäten.

Bedrohungsarten für die Interprozesskommunikation in Netzen (Forts.)

➢ **Aktive Angriffe** : aktive Beeinträchtigung des Nachrichtenflusses durch Eindringling

- **Modifikation des Nachrichtenflusses** : Wiederholung, Umordnung, Löschen und Einfügen von Nachrichten; bei Änderung der Protokollkontrollinformation
  → evtl. Umleitung des Stroms an falschen Adressaten

- **Verhinderung oder Verzögerung der Auslieferung von Nachrichten**
  an Empfänger :
  Nachrichten des gesamten Stroms gelöscht oder temporär zwischengespeichert

- **Maskerade** : Vorspiegeln einer falschen (Benutzer-, Prozess-) Identität einem Kommunikationspartner gegenüber oder bei Zugriffen auf Ressourcen.

⇒ **Entwurfsziele** für Mechanismen zur Gewährleistung von Sicherheit bei Kommunikation :

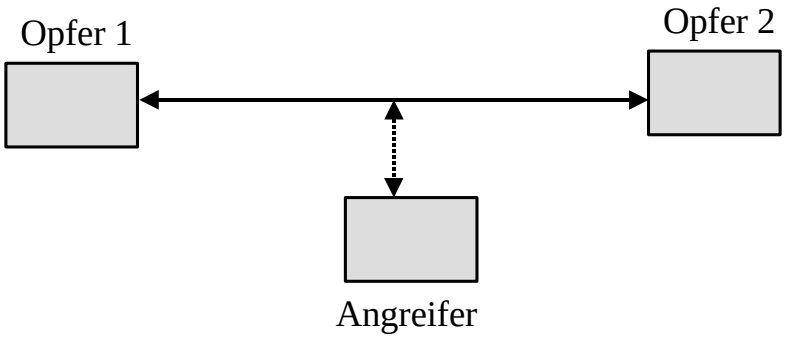
1) Verhinderung passiver Angriffe, z.B. durch Datenverschlüsselung

2) Entdeckung aktiver Angriffe und Beseitigung ihrer negativen Auswirkungen, z.B. auch hier durch Verschlüsselung und Identitätskontrollmechanismen.

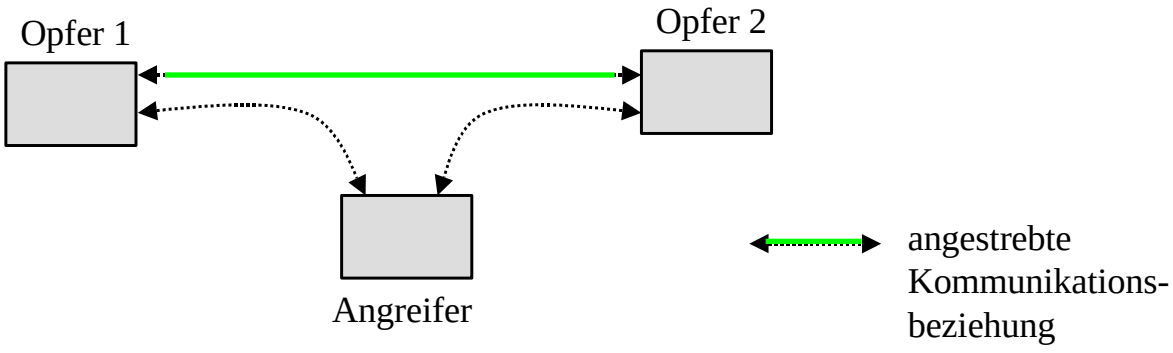
Spezielle Angriffstechniken in Kommunikations- und Rechnernetzen

- **Abhören des Netzverkehrs** (″**Wiretapping**″)

a) **Passives Wiretapping** (auch : ″**Sniffing**″)



b) **Aktives Wiretapping** (auch : ″**Man in the Middle**″ -Angriff)



Spezielle Angriffstechniken in Kommunikations- und Rechnernetzen (Forts.)

- **"Spoofing"/Maskerade**
  → Fälschen der Absenderadresse einer Dateneinheit (z.B. eines IP-Pakets), insbesondere zur Verschleierung der wahren Identität und zur Vortäuschung der Identität eines vertrauenswürdigen Kommunikationspartners

- **"Hijacking"**
  → Übernahme eines Endpunktes einer Verbindung, insbesondere um Rolle des bisherigen Kommunikationspartners (vom Opfer unbemerkt) in zukünftiger Kommunikation zu übernehmen

- **"Denial-of-Service" (DoS)**
  → Unbefugtes Aufbrauchen der Betriebsmittel eines Rechners, insbesondere
  - CPU-Belegung durch unerlaubtes Ausführen von Programmen (z.B. „Überfluten“ eines Server-Rechners mit Anfragen seitens eines Angreifers)
  - Übertragungsleistung durch „Überfluten“ des Rechners mit Nachrichten
  - Belegung von Speicherplatz auf Festplatte

  Besonders (heim-)tückisch : ***Distributed Denial-of-Service***
  (kooperativer DoS-Angriff zahlreicher Angreifer im Netz)

Erreichen von Datenschutz durch:

➢ Legislative Maßnahmen	→	Datenschutzgesetze
➢ Organisatorische Maßnahmen	→	Zugangskontrolle (Raum, Gerät)
➢ Identitätskontrolle	→	Password,...
➢ Zugriffskontrolle	→	nur Datenbankausschnitt sichtbar, capabilities, ...
➢ Kryptographie/ Datenverschlüsselung	→	Chiffrierverfahren

Schutz auf verschiedenen Schichten einer Rechnernetzarchitektur:

- auf *Datensicherungsebene*: geringer Aufwand, geringer Schutz
  - •
  - •
  - •
- auf *Anwendungsebene*: hoher Aufwand, Schutz im gesamten Kommunikationssystem

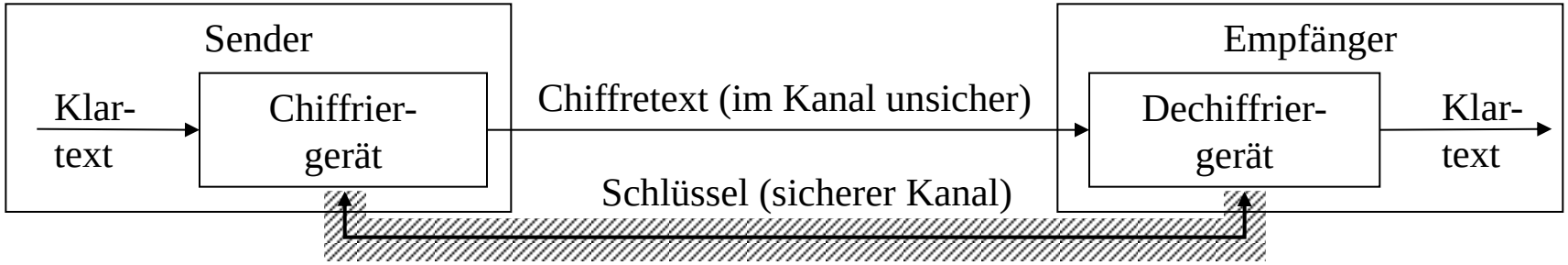
12.2 Chiffrierverfahren und ihr Einsatz zur Sitzungsverschlüsselung

Chiffrierverfahren:

- **Symmetrisch** : gleicher Schlüssel S für A und B
  $\mathbf{E_S\,(V_S\,(M))\;=\;M}$ $\qquad\forall M \mid M = \text{Nachricht}$
  E_S/V_S : Entschlüsselung/Verschlüsselung mit S
  Bsp.: **D**ata **E**ncryption **S**tandard (**DES**); DES-Chips existieren bereits seit langem

- **Asymmetrisch** : Schlüssel S existiert zum Verschlüsseln
  Schlüssel S‘ existiert zum Entschlüsseln $(S \neq S')$
  $\mathbf{E_{S'}\,(V_S\,(M))\;=\;M}$ $\qquad\forall M \mid M = \text{Nachricht}$
  Bem.: Veröffentl. von S möglich, S‘ geheim !!
  → ***„public key“-Verfahren***
  Bsp.: **R**ivest-**S**hamir-**A**dleman-Verfahren (**RSA**)

Kommunikation unter Benutzung von Chiffrierverfahren:



DES (**D**ata **E**ncryption **S**tandard) als Beispiel eines symmetr. Chiffrierverfahrens

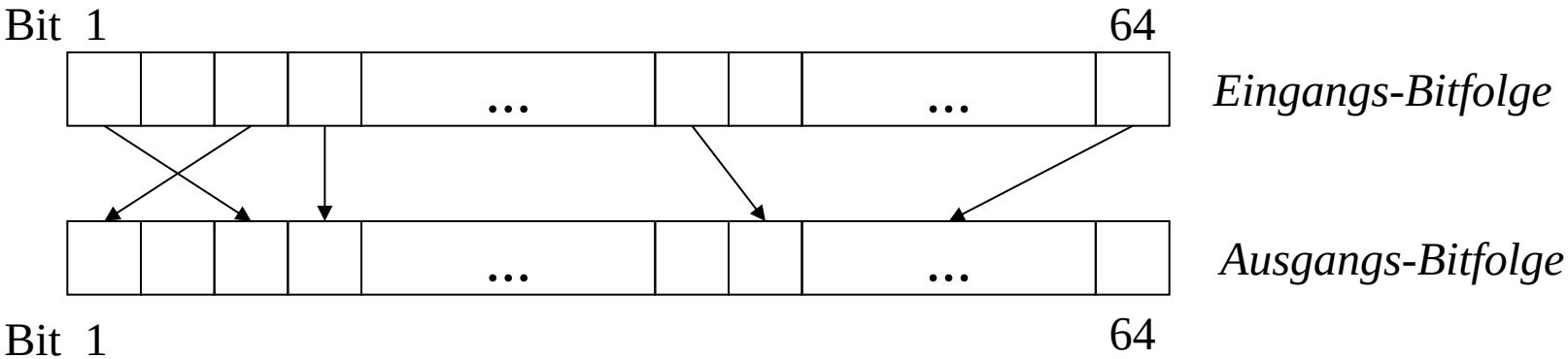
Ziel: Verschlüsselung von (Daten-)Blöcken *fester* Länge (64 Bit)
→ Nachrichten in Blöcken à 64 Bit zu zerlegen und Blöcke einzeln zu verschlüsseln

Vorgehensweise bei DES-Verschlüsselung:

- Vorauss.: S ∧ E besitzen *identischen* 56-Bit DES-Schlüssel
  (entspr. ~ 10^{17} mögl. Schlüsselwerte)
  → aus DES-Schlüssel werden 16 Unterschlüssel generiert.

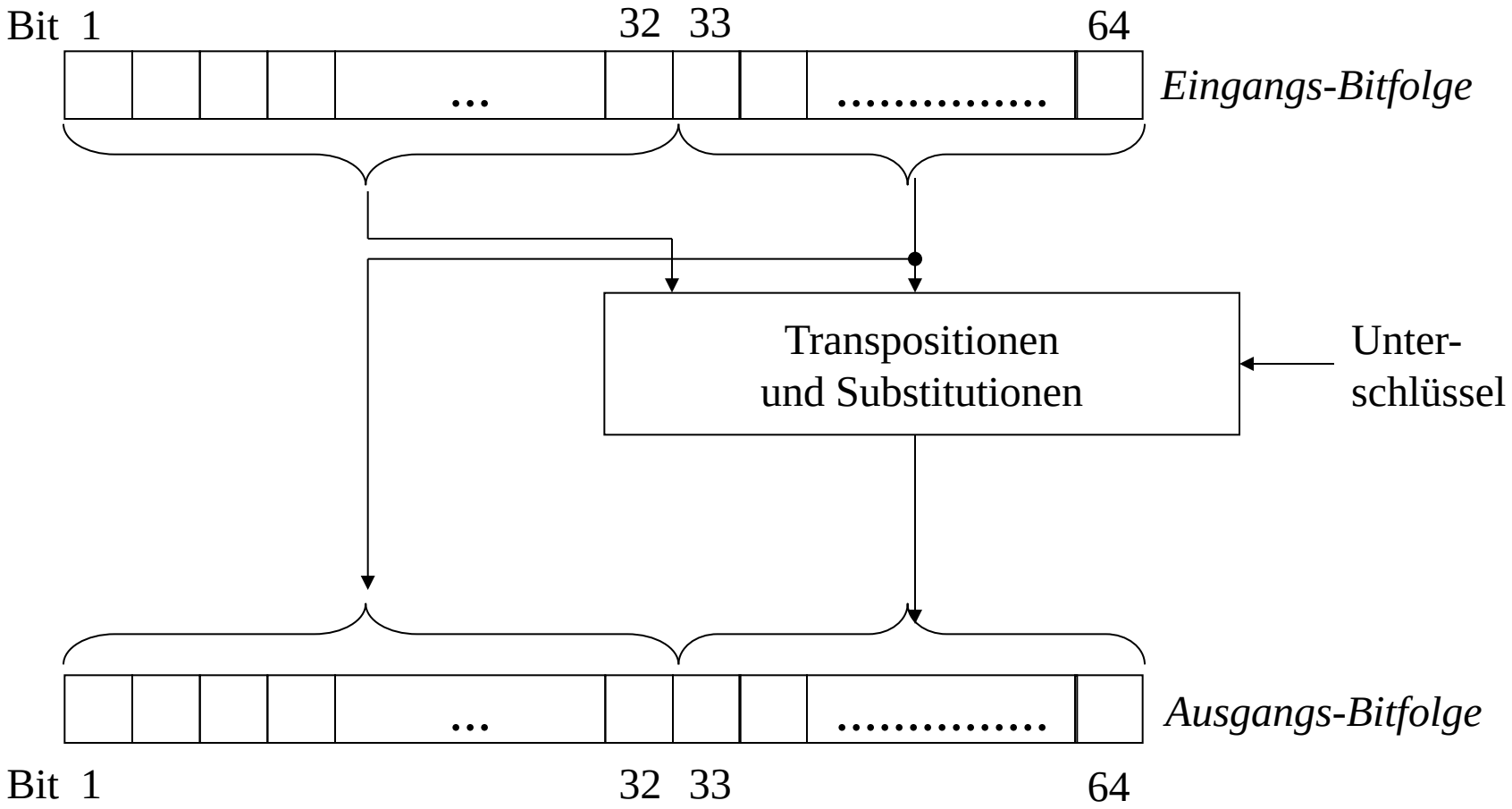
- **Operationstypen**:
  - **Transposition**: Umordnung der Bits eines Blocks

Bsp.:

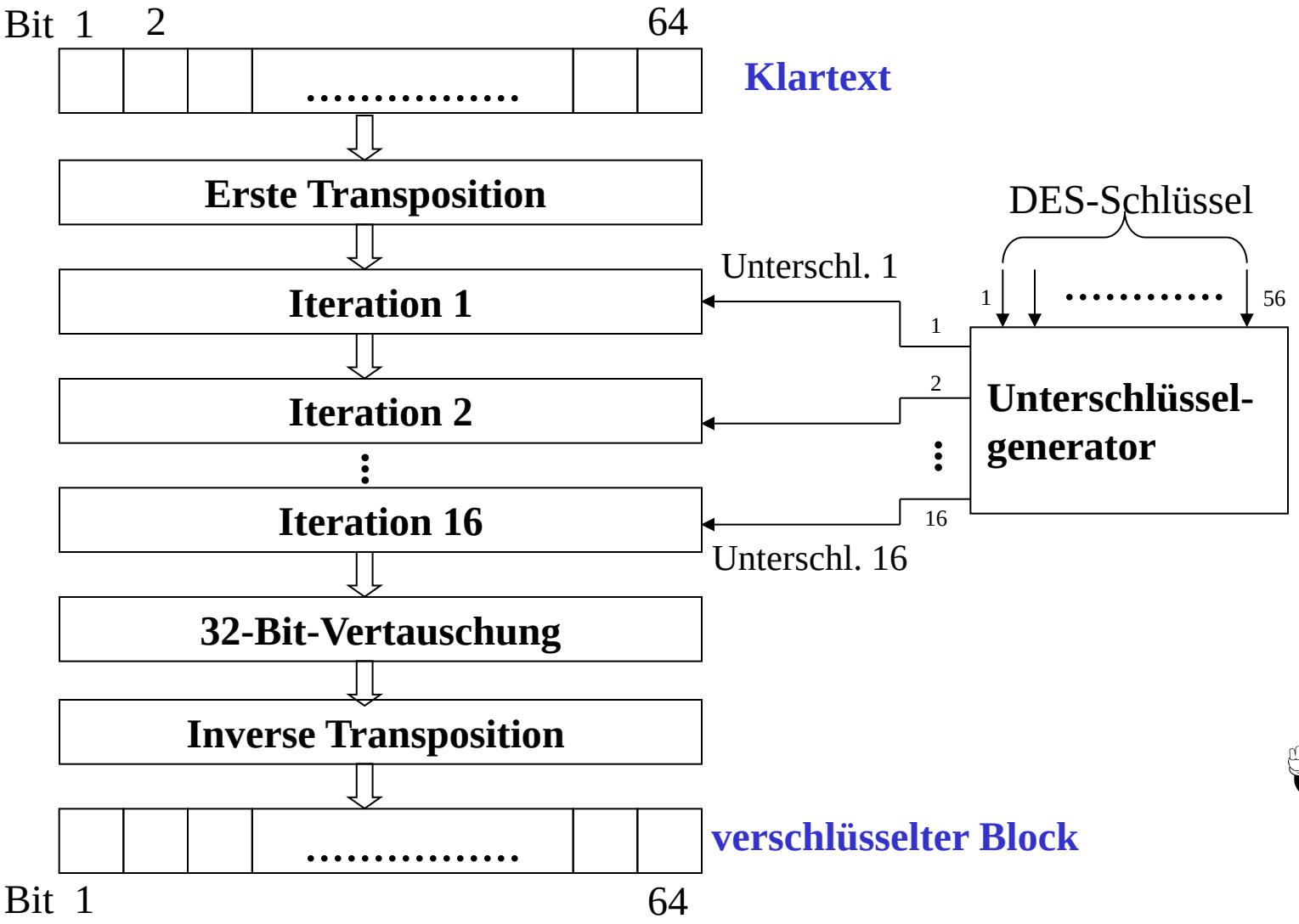


– **Substitution**:
(Schlüsselabhängige) Ersetzung einer gegebenen Bitfolge durch eine neue Bitfolge

Bsp.: Iteration (bei DES)



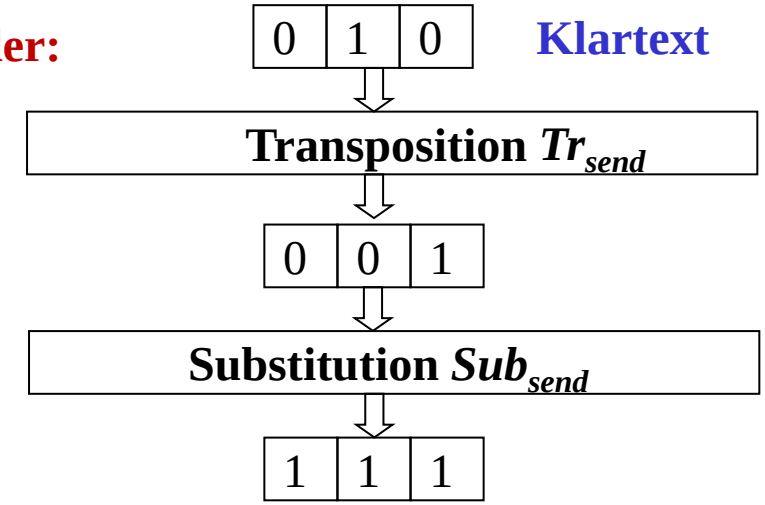
- Bei DES-Verschlüsselung gewählte Kombination von Transpositions- und Substitutionsoperationen:

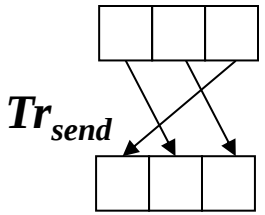


Bem.: Bei Entschlüsselung → umgekehrte Sequenz der Operationen

Elementares Beispiel : Verschlüsselung von 3 Bit mit Transposition gefolgt von Substitution

Sender:

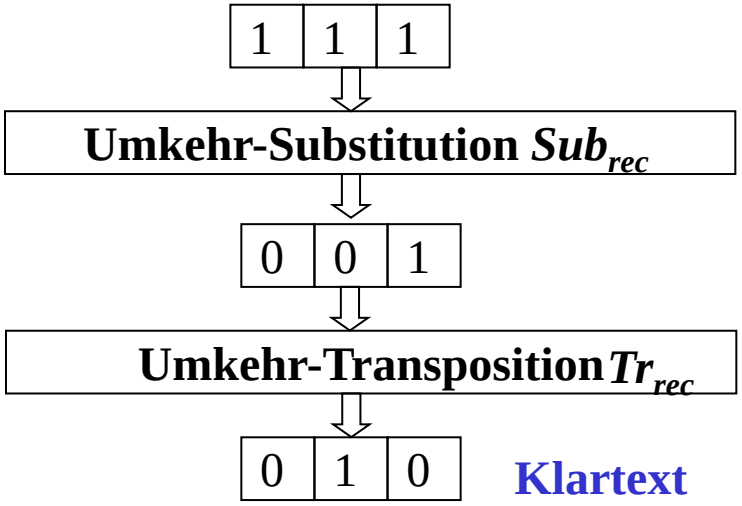


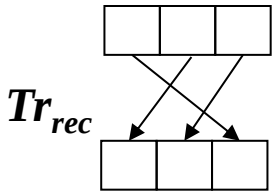


Substitutionstabellen:

Sub_{send} :	Sub_{rec} :
$0_{10} \rightarrow 5_{10}$	$0_{10} \rightarrow 3_{10}$
$1_{10} \rightarrow 7_{10}$	$1_{10} \rightarrow 5_{10}$
$2_{10} \rightarrow 4_{10}$	$2_{10} \rightarrow 7_{10}$
$3_{10} \rightarrow 0_{10}$	$3_{10} \rightarrow 4_{10}$
$4_{10} \rightarrow 3_{10}$	$4_{10} \rightarrow 2_{10}$
$5_{10} \rightarrow 1_{10}$	$5_{10} \rightarrow 0_{10}$
$6_{10} \rightarrow 6_{10}$	$6_{10} \rightarrow 6_{10}$
$7_{10} \rightarrow 2_{10}$	$7_{10} \rightarrow 1_{10}$

Empfänger:



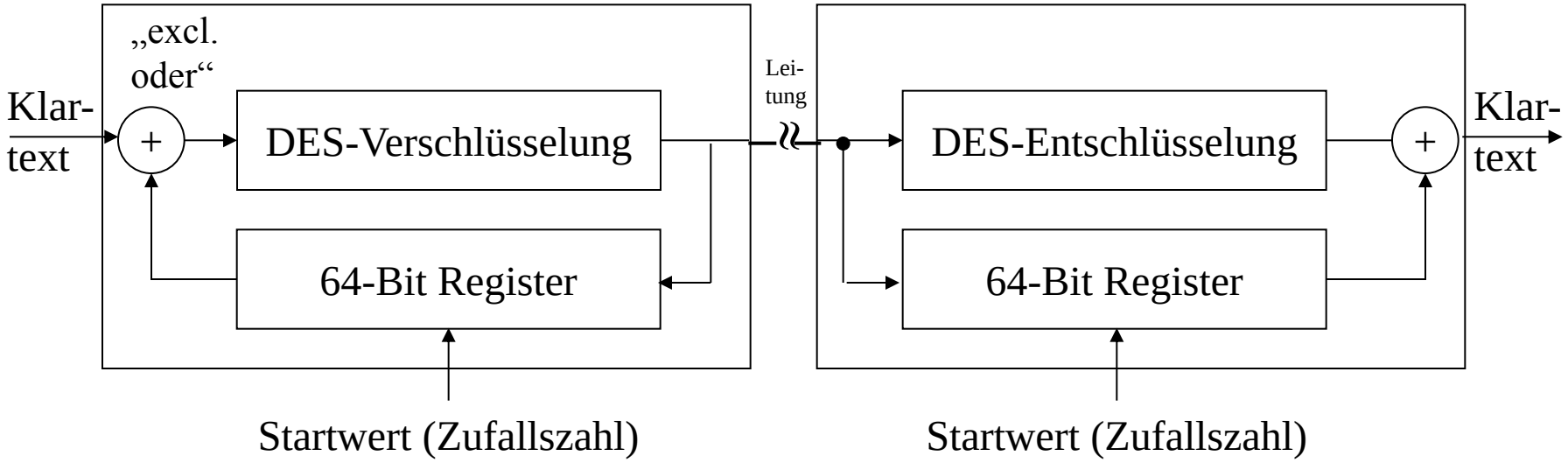


Probleme der direkten DES-Benutzung bei Verschlüsselung zu übertragender Daten:

a) Erkennung folgender Fehler schwierig bzw. unmöglich:
- Einfügen eines korrekt verschlüsselten Blockes
- Löschen eines Blockes
- Ersetzen eines Blockes durch einen anderen (korrekt verschlüsselten)

b) Erleichterte Schlüsselentdeckung bei häufig wiederkehrender Klartext-Bitfolge (z.B. 8 × ASCII-codiertes „ *blank* “)

→ Ausweg: „*Chaining*“ bzw. *DES-CBC-Modus* (CBC ≅ Chain Block Cipher)



c) Ursprüngliche Schlüssellänge (56 Bit) inzwischen viel zu gering; daher z.B. *Triple DES* (auch: *3DES*) mit Schlüssellänge von 3x56 = 168 Bit (de facto 112 Bit)

Symmetrische Chiffrierverfahren zur Sitzungsverschlüsselung

Beispiel I : Verschlüsselung einer Sitzung zwischen Prozessen A und B (Schlüsselverteilungszentrale Z; Z hat Schlüssel S_A bzw. S_B gemeinsam mit A bzw. B)

Symmetr. Chiffrierverfahren :

(1) A → Z : $V_{S_A}(A, B, id_A)$ {Z erhält Adr. von A, B sowie eindeutige Sitzungskennung }

in Z : $E_{S_A}(V_{S_A}(A, B, id_A)) = (A, B, id_A)$

(2) Z → A : $V_{S_A}(id_A, B, S_S, V_{S_B}(S_S, A, id_A))$ {S_S = Sitzungsschlüssel}

in A : S_S gegeben durch $E_{S_A}(V_{S_A}(id_A, B, S_S, ...))$ }

(3) A → B : $V_{S_B}(S_S, A, id_A)$ {B erhält Sitzungsschlüssel}

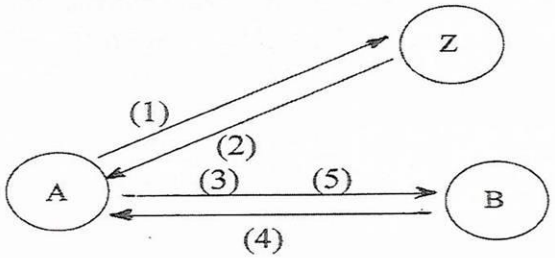
in B : S_S gegeben durch $E_{S_B}(V_{S_B}(S_S, A, id_A))$

(4) B → A : $V_{S_S}(id_A, id_B)$

in A : $E_{S_S}(V_{S_S}(id_A, id_B)) = (id_A, id_B)$ {B kennt Kommunikationspartner A und S_S}

(5) A → B : $V_{S_S}(id_B)$

in B : $E_{S_S}(V_{S_S}(id_B)) = (id_B)$ {letzte Quittung; Nachricht in (4) wurde nicht „abgefangen"}



Bem. : nur Sitzungsschlüssel wird übertragen (verschlüsselt)

Asymmetrische Chiffrierverfahren zur Sitzungsverschlüsselung

Beispiel II : Verschlüsselung einer Sitzung zwischen A und B
(Schlüsselverteilungszentrale Z;
Z kennt öffentl. Schlüssel S_A bzw. S_B von A bzw. B;
A und B kennen a priori den geheimen Schlüssel $\overline{S_Z}$ von **Z zum Verifizieren)**

Nota bene: Öffentl. Schlüssel der Komm.-Partner durch Signatur von Z beglaubigt ! Z veröffentlicht überdies NICHT den Schlüssel S_Z !

Asymmetr. Chiffrierverfahren :

(1) A → Z : (A, B, id_A) {Z erhält Adr. von A, B sowie eindeutige Sitzungskennung}

(2) Z → A: $V_{S_Z}(id_A, S_B, B)$ {Z liefert öffentl. Schlüssel S_B von B}
in A : $E_{\overline{S_Z}}(V_{S_Z}(id_A, S_B, B)) = (id_A, S_B, B)$

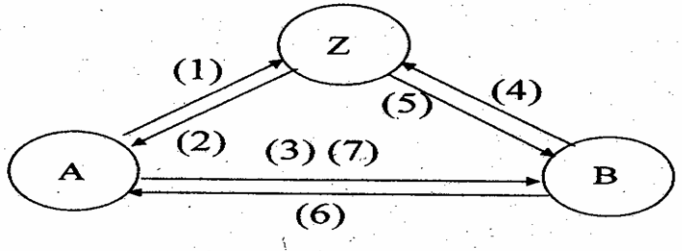
(3) A → B : $V_{S_B}(id_A, A)$ {für Kommunikation mit B verwendet A : S_B}
in B : $E_{\overline{S_B}}(V_{S_B}(id_A, A)) = (id_A, A)$

(4) B → Z : (B, A, id_B) {B kontaktiert Z (wegen S_A)}

(5) Z → B : $V_{S_Z}(id_B, S_A, A)$ {Z liefert öffentl. Schlüssel S_A von A}
in B : $E_{\overline{S_Z}}(V_{S_Z}(id_B, S_A, A)) = (id_B, S_A, A)$

(6) B → A : $V_{S_A}(id_A, id_B)$ {für Kommunik. mit A verwendet B : S_A}
in A : $E_{\overline{S_A}}(V_{S_A}(id_A, id_B)) = (id_A, id_B)$ {B kennt Komm.-partner A}

(7) A → B : $V_{S_B}(id_B)$
in B : $E_{\overline{S_B}}(V_{S_B}(id_B)) = (id_B)$ {letzte Quittung; Nachricht in (6) wurde nicht „abgefangen"}



Bem. : nur öffentliche Schlüssel werden übertragen (verschlüsselt)

12.3 Sicherheitsmechanismen und -dienste

Sicherheitsdienste für (offene) verteilte Systeme

vgl. u.a.
- -- Trusted Computer System Evaluation Criteria (TCSEC) des National Computer Security Center (NCSC); abgelöst durch Common Criteria Standard
- -- OSI Secure Protocol Reference Model

-- ***Peer entity authentication***: Authentifikation von Kommunikationspartnern (u.a. zur Überprüfung von Zugriffsberechtigungen auf Daten und sonstige BM)

-- ***Data origin authentication***: Authentifikation der Datenquelle (u.a. Senderidentität korrekt ? → Maskerade verhindern)

-- ***Access control service***: Schutz der BM (Kommunikations-BM, Daten, Verarbeitungs-BM) vor unberechtigten Zugriffen (absichtlich oder unabsichtlich)

-- ***Confidentiality***: Vertraulichkeit bei Datenaustausch
→ erreichbar u.a. durch Verschlüsselung der Daten

-- ***Traffic flow confidentiality***: Vertraulichkeit für Kommunikationsverhalten
→ wer kommuniziert mit wem ? ... wann ? ... wie intensiv ?

-- ***Data integrity***: Wahrung der Datenintegrität, d.h. Schutz der Daten vor aktiven Angriffen (s.o.), u.a. bei verbindungsloser Kommunikation (Schutz einzelner PDUs vor Modifikation, Zerstörung, etc.) und bei verbindungsorientierter Kommunikation (Schutz der gesamten über die Verbindung ausgetauschten Sequenz von PDUs)

-- ***Non-repudiation***: Senden und Empfangen für eine gegebene Dateneinheit a posteriori nachweisbar („leugnen zwecklos"!)

Sicherheitsmechanismen

1. **Encryption** – based on encryption algorithms;
   - Link encryption
   - End-to-end encryption
   - Symmetric cryptosystems
   - Public-key cryptosystems
   - Key management

2. **Digital signature** – requires two procedures: signing the data unit, and verifying a signed data unit;

3. **Access control** – based on the identity of an entity to determine its access rights;
   - Access control lists
   - Passwords
   - Capability lists
   - Credentials
   - Labels

4. **Data integrity** – requires the sender to append to a data unit additional information which is a function of the data itself;
   - Checksums, for example, a block check code, or a cryptographic checkvalue, which may be encrypted
   - Sequencing and/or timestamping

5. **Authentication** – proves the identity of the entity;
   - Cryptographic means
   - Passwords

6. **Traffic padding** – to provide various levels of protection against traffic analysis;

7. **Routing control** – by which routes are chosen dynamically or statically so as to use only physically secure networks, links, etc.;

8. **Notarization** – gives assurance of some properties of the data communicated such as its origin, integrity, time, and destination; this mechanism is provided by a third party notary which is trusted by communicating entities.

List 12.1 List of service mechanisms.

Zusammenhänge zwischen Sicherheitsdiensten und -mechanismen

Service	Security mechanism							
	1	2	3	4	5	6	7	8
Peer entity authentication	C	B	n	n	Y	n	n	n
Data origin authentication	C	B	n	n	n	n	n	n
Access control service	C	n	Y	n	n	n	n	n
Confidentiality	Y	n	n	n	n	n	Y	n
Traffic flow confidentiality	A	n	n	n	n	A	Y	n
Data integrity	C	B	n	Y	n	n	n	n
Non-repudiation	C	Y	n	A	n	n	n	A

Notation:

Y -- Mechanismus ist geeignet
n -- Mechanismus ist nicht geeignet
A -- simultan zu benutzen, um Dienst zu erbringen
B -- Mechanismus der mehr liefert als benötigt wird
C -- Mechanismus der in Verbindung mit einem anderen genutzt werden kann, um Dienst zu erbringen

Plazierung der Sicherheitsdienste im ISO/OSI-Architekturmodell

OSI Layer 1	2	3	4	5	6	7	Service
		X X	X X			X X	1. IDENTIFICATION/AUTHENTICATION - Data origin (Connectionless) - Peer entity (Connection)
		X X	X X			X X	2. ACCESS CONTROL User agent authorization - Peer entity authorization
		X X X	X X X			X X X X	3. INTEGRITY Connection integrity with recovery - Connection integrity without recovery - Selective field connections integrity - Connectionless integrity
X X	X X	X X X	X X			X X X X	4. CONFIDENTIALITY Connection - Connectionless - Selective field - Traffic flow
						X X	5. NON-REPUDIATION Originator - Recipient

OSI Layer:
1 : **Physical** L./ Physikalische Schicht
2 : **Data Link** L./ Datensicherungs-
3 : **Network** L./ Netzwerk-
4 : **Transport** L./ Transport-
5 : **Session** L./ Sitzungs-
6 : **Presentation** L./ Darstellungs-
7 : **Application** L./ Anwendungs-

:

ad 1

Data origin (connectionless oriented) authentication :
Authentifikation des Senders von Daten.
Peer entity (connection oriented) authentication :
Authentifikation des Kommunikationspartners während der Datenaustauschphase.

ad 2

Access control :
Verhinderung eines nicht-authorisierten Zugriffs auf BM.

ad 3

Connection integrity (with and without error recovery) :
Entdeckung jeglicher Art von Veränderung einzelner Dateneinheiten oder einer Sequenz von Daten.
Selective field connectionless integrity :
Schutz ausgewählter Felder innerhalb einer Dateneinheit.
Connectionless integrity :
Schutz einzelner Dateneinheiten bei verbindungsloser Kommunikation.

ad 4

Connection (bzw. connectionless) confidentiality :
Gewährleistung der Vertraulichkeit für vollständige Sequenz ausgetauschter Benutzerdaten bzw. der Benutzerdaten innerhalb einer einzigen Nachricht.
Selective field confidentiality :
Gewährleistung der Vertraulichkeit für ausgewählte Felder der Benutzerdaten.

ad 5

Non-repudiation with proof of origin :
Nachweis der Urheberschaft bei Senden von Daten (gegenüber Empfänger).
Non-repudiation with proof of delivery :
Nachweis für Entgegennahme von Daten durch Empfänger (gegenüber Sender).

Elementare Funktionen zur Implementierung der Sicherheitsdienste gemäß ISO/OSI :

authenticate [id; authenticator] {result; status}
verifies that the authenticator does correspond with the claimed id by searching the local Secure Management Information Base and responding with the correct result and status.

authorize [id; type; resource] {result; status}
verifies the authorization of id with the indicated type for access to the requested resource and sets the correct result and status.

encipher [pt; length; keyname] {ct; length; status}
encrypts a message beginning at pt for the indicated length into cryptogram beginning at ct for the indicated length, using the key associated with keyname, and sets the resulting status.

decipher [ct; length; keyname] {pt; length; status}
decrypts a cryptogram beginning at ct for the indicated length into message beginning at pt for the indicated length, using the key associated with keyname, and sets the resulting status.

computemac [data; length; keyname] {mac; status}
computes a Message Authentication Code (mac) on the data of indicated length, using the key associated with keyname, and sets the resulting status.

verifymac [data; length; userid; keyname; mac] {result}
computes a Test Message Authentication Code (tmac) on the data of indicated length, using the key associated with keyname, and sets the correct result to indicate if tmac is identical with the input mac.

sign [data; length; userid; keyname] {signature; status}
computes a signature on the data of indicated length for the user indicated by userid, using the key associated with keyname, and sets the resulting status.

verifysignature [data; length; userid; keyname; signature] {result; status}
computes a Test Signature (signature) on the data of indicated length for the user indicated by userid, using the key associated with keyname, compares it with signature, and sets the correct result and status.

List 12.2 Primitive functions to implement ISO/OSI security services (adapted from (Branstad 1986)).