Encryption-Based Security

Use encryption methods to

- prevent eavesdropping of messages
- prevent tampering with messages
- prevent masquerading and replay attacks

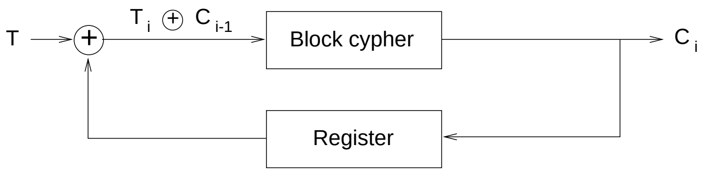
Cryptography

- $E(K_E, T) = E_{K_E}(T) = \{T\}_{K_E}$: encryption of message T with key K_E
- $D(K_D, T) = D_{K_D}(T) = \{T\}_{K_D}$: decryption of message T with key K_D
- $D(K_D, E(K_E, T)) = T$ for *cognate* (matching) keys K_D, K_E
- $E(K_E, T) \to T$ is "unfeasible" without knowledge of K_D
- usually algorithms E, D well known
- cipher should be resilient to
  - ciphertext only attacks
  - known plaintext attacks
  - chosen plaintext attacks
  - guessing of keys

  in general only have "practically" (computationally) secure ciphers

Block vs. stream ciphers

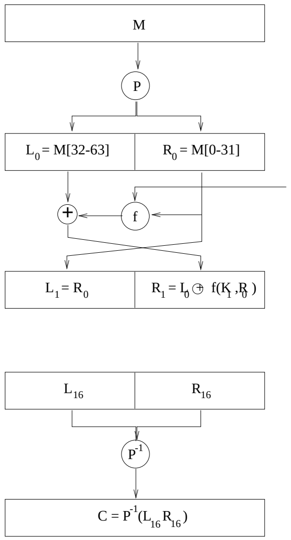
- block cyphers
  - works on a fixed-size block at a time
  - easier to implement
  - needs padding on last block (compromise?)
- stream cipher
  - works on stream of bits, encryption depends on previous bit(s)
  - tends to be stronger
  - if part of stream is lost, rest is undecipherable



Symmetric Cryptosystems: $K_D = K_E$

- also called *private key* encryption
- fast
- need one pair of keys for each pair of agents
- need secure channel to establish key
- examples: Enigma, UNIX crypt, DES (data encryption standard)

DES Encryption



- P: initial permutation
- K_i: 56-bit key, rotated 1–2 bits each step
- f:
  - transpose/duplicate bits of R yielding 48 bits
  - XOR with key
  - substitute/reduce number bits to 32
- vanilla DES no longer considered safe against brute-force attack
- use e.g. triple DES
  total key length = 168 bits

National Bureau of Standards: *Data Encryption Standard (DES)*. Number 46 in Federal Information Processing Standards. Washington DC, 1977.

Public key encryption

RSA algorithm:

1. choose two primes $P, Q > 10^{100}$
2. $N = PQ; Z = (P-1)(Q-1)$
3. choose K_E relatively prime with Z
4. determine K_D such that $K_E K_D = 1 \bmod Z$
5. encrypt k bits, $2^k < N$: $\{T\}_{K_E} = TK_E \bmod N$
6. decrypt k bits: $\{C\}_{K_D} = C^{K_E} \bmod N$

$\{\{T\}_{K_E}\}_{K_D} = \{\{T\}_{K_D}\}_{K_D} = T \; \forall T : 0 \leq T \leq N$

R.L. Rivest, A. Shamir, and L. Adleman: A method for obtaining digital signatures and public-key cryptosystems. *Comm. ACM*, 21:120–126, 1978.

Features & limitations

- can publish one key, K_P, keeping the other, K_p secret
- security depends on factoring large numbers being computationally hard
- easy to establish secure channel
- much slower than symmetric systems
  ⇒ use to establish symmetric key pair
- can use for digital signature:
  sign message T by appending $S = \{h(T)\}_{K_p}$,
  h is well-known hash (*digest*)
  receiver can validate by verifying that $h(T) = \{S\}_{K_P}$
  validates sender as well as message

Digests

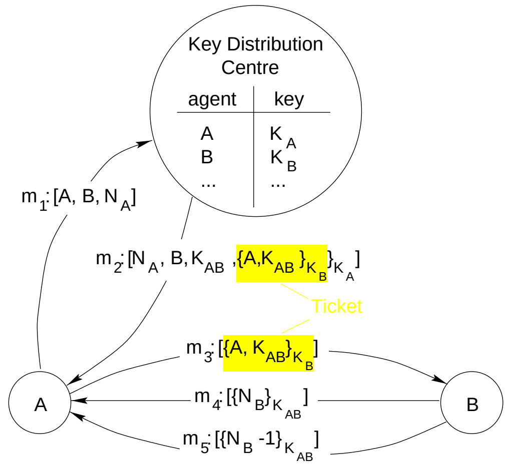
- Digital signature relies on digest being cryptographically secure (also called *secure checksum*):
- given $D(M)$ must be computationally infeasible to construct a message M' so that $D(M') = D(M)$
- example: MD5 [Rivest 1992]:
  essentially XORs message and some constants in blocks of 128 bits

Key distribution: Symmetric keys

- central *key distribution centre* D
- each agent A shares a (symmetric) key K_A with D
- A wants to communicate with B:
  1. $[A \to D, B, N_A]$, N_A is unique id (*nounce*)
  2. $[D \to A, \{N_A, B, K_{AB}, \{A, K_{AB}\}_{K_B}\}_{K_A}]$,
     $\{A, K_{AB}\}_{K_B}$ is called a *ticket*
  3. $[A \to B, \{A, K_{AB}\}_{K_B}]$
  4. $[B \to A, \{N_B\}_{K_{AB}}]$, *challenge*
  5. $[A \to B, \{N_B - 1\}_{K_{AB}}]$

R.M. Needham and M.D. Schroeder: Using encryption for authentication in large networks of computers. *Comm. ACM*, 21:993–999, 1978.

Key distribution: Symmetric keys...

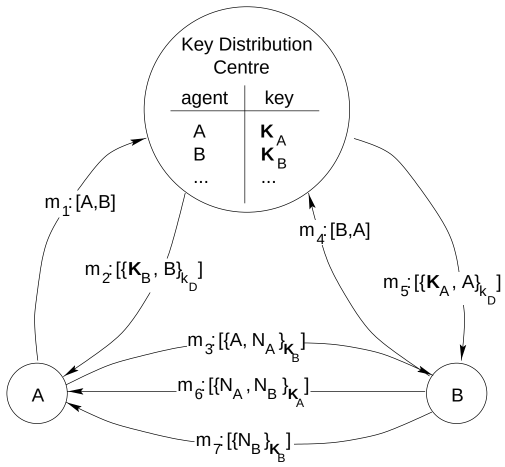


Key distribution: Public keys

- central *key directory* D
- all agents know D's public key $\mathbf{K}_D$, k_D is D's private key
- A wants to communicate with B:
  1. $[A \to D, B]$
  2. $[D \to A, \{\mathbf{K}_B, B\}_{k_D}]$
  3. $[A \to B, \{A, N_A\}_{\mathbf{K}_B}]$
  4. $[B \to D, A]$
  5. $[D \to B, \{\mathbf{K}_A, A\}_{k_D}]$
  6. $[B \to A, \{N_A, N_B\}_{\mathbf{K}_A}]$
  7. $[A \to B, \{N_B\}_{\mathbf{K}_B}]$

Needham, Schroeder, 1978

Key distribution: Public keys...



Pretty Good Privacy (PGP)

"Cryptography for the masses" by Philip Zimmermann

- free system supporting encryption, authentication, key management, digital signatures
- easy to install and use
- based on RSA implementation
- supposedly as strong as any known civil cryptosystem
- available world-wide after "illegal" export from US (considered "munition")
  court case against Zimmermann for illegal export unsuccessful
- restricted in US and Canada due to RSA patent

Kerberos

Commercial authentication system developed at MIT
J. Steiner, C. Neuman, and J. Schiller: Kerberos: An authentication service for open network systems. Berkeley, CA, USA, 1988.

- Kerberos KDC contains *authentication service* (A) and *ticket granting service* (T)
- KDC contains passwords of all authorised users
- at login user enters name and password to local login program which obtains from A a session key including a ticket for T:
  1. $[C \rightarrow A, T, n]$, n is a nounce
  2. $[A \rightarrow C\{K_{CT}, n\}_{K_C}, \{< C, T >\}_{K_T}]$,
     $< C, T >= [C, T, t_1, t_2, K_{CT}]$ is *ticket* valid between t_1 and t_2

  C's password is not send across the network and can be erased once the ticket has been obtained.

Kerberos...

To obtain a service from S, C first gets a ticket from T:

3. $[C \rightarrow T, \{C, t\}_{K_{CT}}, \{< C, T >\}_{K_T}, S, n]$, C, t is *authenticator*
4. $[T \rightarrow C, \{K_{CS}, n\}_{K_{CT}}, \{< C, S >\}_{K_S}]$,
5. $[C \rightarrow S, \{C, t\}_{K_{CS}}, \{< C, S >\}_{K_S}, \mathit{request}, n]$
6. $[S \rightarrow C, \mathit{reply}, \{n\}_{K_{CS}}]$

[1] National Bureau of Standards. *Data Encryption Standard (DES)*. Number 46 in Federal Information Processing Standards. US NBS, Washington DC, 1977.

[2] R.L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Comm. ACM*, 21:120–126, 1978.

[3] R.L. Rivest. The MD5 message-digest algorithm. Technical Report RFC 1321, Network Working Group, MIT, April 1992. Available from URL ftp://nic.ddn.mil/rfc/rfc1321.txt.

[4] R.M. Needham and M.D. Schroeder. Using encryption for authentication in large networks of computers. *Comm. ACM*, 21:993–999, 1978.

[5] J. Steiner, C. Neuman, and J. Schiller. Kerberos: An authentication service for open network systems. In *Proc. 1988 Winter USENIX Conf.*, Berkeley, CA, USA, 1988.