Tinklo saugumas

Saugumas

- Poreikis: IP Protokolas neturi mechanizmo užtrikrinti saugumui žemesniuose lygiuose
- Šifravimas simetriniu raktu
- Šifravimas viešuoju raktu
- Skaitmeniniai parašai

Šifravimas simetriniu raktu

Cipher	Author	Key length	Comments
Blowfish	Bruce Schneier	1–448 bits	Old and slow
DES	IBM	56 bits	Too weak to use now
IDEA	Massey and Xuejia	128 bits	Good, but patented
RC4	Ronald Rivest	1–2048 bits	Caution: some keys are weak
RC5	Ronald Rivest	128–256 bits	Good, but patented
Rijndael	Daemen and Rijmen	128–256 bits	Best choice
Serpent	Anderson, Biham, Knudsen	128–256 bits	Very strong
Triple DES	IBM	168 bits	Second best choice
Twofish	Bruce Schneier	128–256 bits	Very strong; widely used

Šifravimas viešuoju raktu

- D(E(P)) = P
- Labai sudėtinga iš E gauti D
- E negali būti palaužtas naudojant atviro teksto ataką
- RSA

RSA

- Parenkami du dideli pirminiai skaičiai p ir q (1024 bitų ilgio)
- $n = p * q$ ir $z = (p - 1)(q - 1)$
- Pasirinkti skaičių d, kuris būtų tarpusavyje pirminis su z
- Ir surasti skaičių e, kur $e * d = 1 \bmod z$

- Šifravimas:

  $C = P^e \pmod n$

- Dešifravimas:

  $P = C^d \pmod n$

- Privatų raktą sudaro pora (d,n)
- Viešą raktą sudaro (e,n)

RSA

Plaintext (P)			Ciphertext (C)		After decryption	
Symbolic	Numeric	P^3	P^3 (mod 33)	C^7	C^7 (mod 33)	Symbolic
S	19	6859	28	13492928512	19	S
U	21	9261	21	1801088541	21	U
Z	26	17576	20	1280000000	26	Z
A	01	1	1	1	01	A
N	14	2744	5	78125	14	N
N	14	2744	5	78125	14	N
E	05	125	26	8031810176	05	E

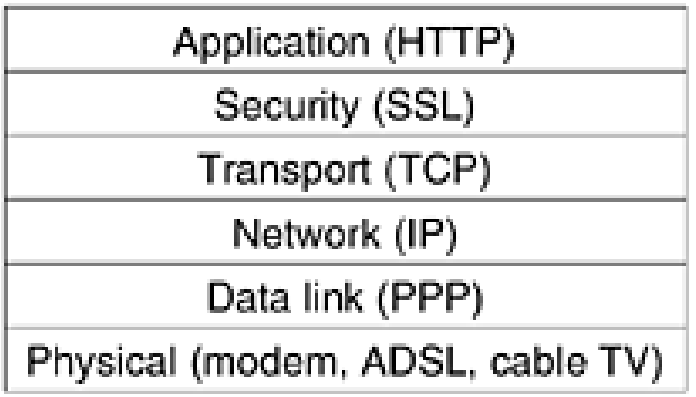
Sender's computation

Receiver's computation

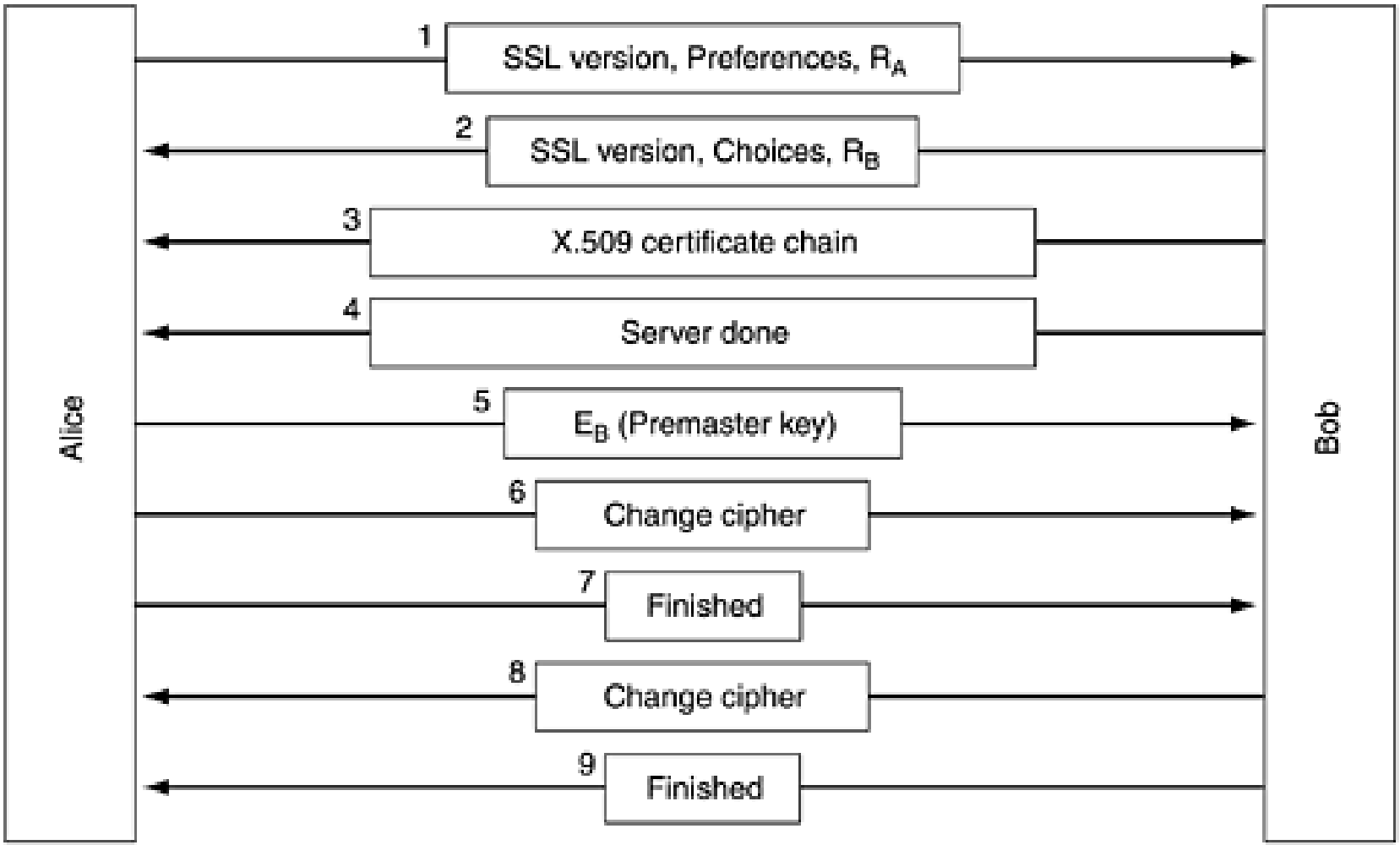
Skaitmeninis parašas

SSL

- Secure Sockets Layer



SSL


Alice
Bob
1
SSL version, Preferences, R_A
2
SSL version, Choices, R_B
3
X.509 certificate chain
4
Server done
5
E_B (Premaster key)
6
Change cipher
7
Finished
8
Change cipher
9
Finished