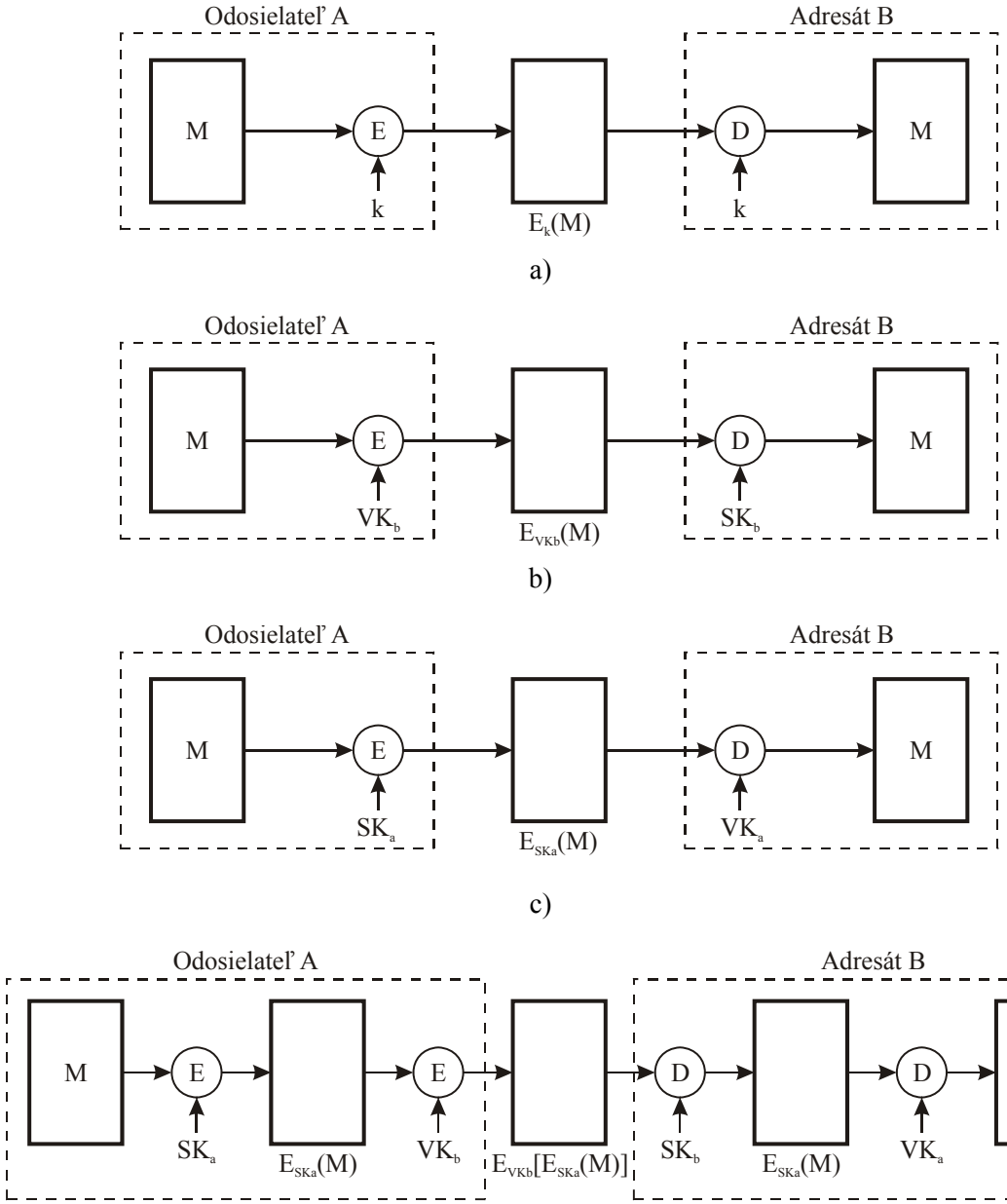
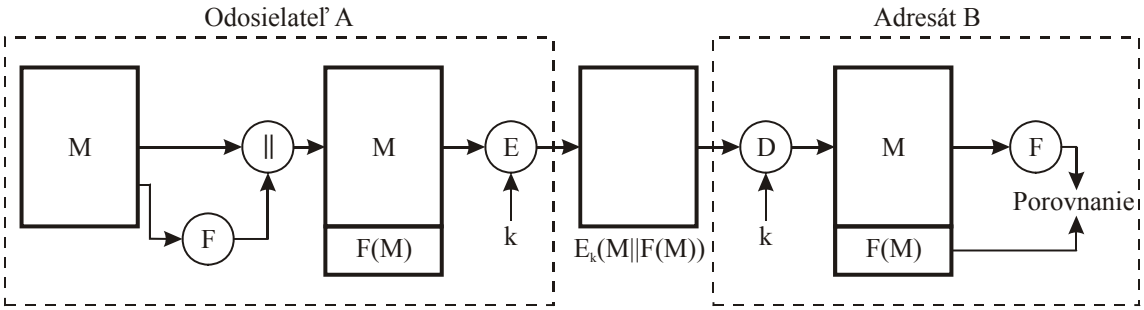
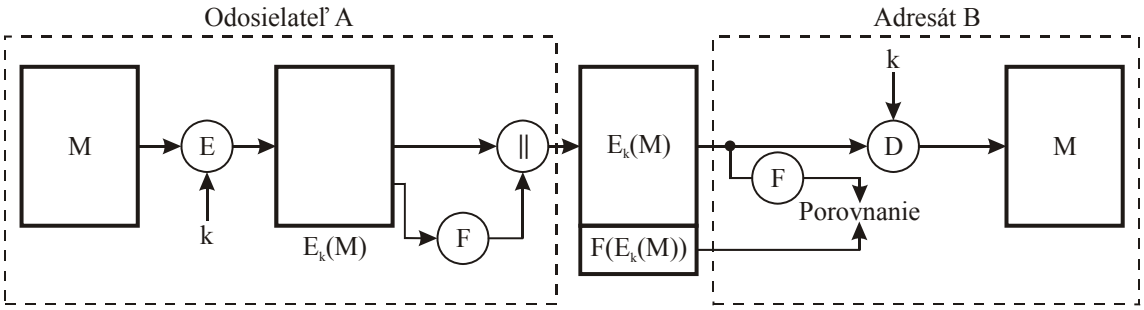
9 AUTENTIZÁCIA POUŽÍVATEĽOV A AUTORIZÁCIA DÁT



Obr. 9.1 Šifrovanie a dešifrovanie správy
a) Symetrické šifrovanie: utajenie a autentizácia
b) Asymetrické šifrovanie: utajenie
c) Asymetrické šifrovanie: autentizácia a podpis
d) Asymetrické šifrovanie: utajenie, autentizácia a podpis

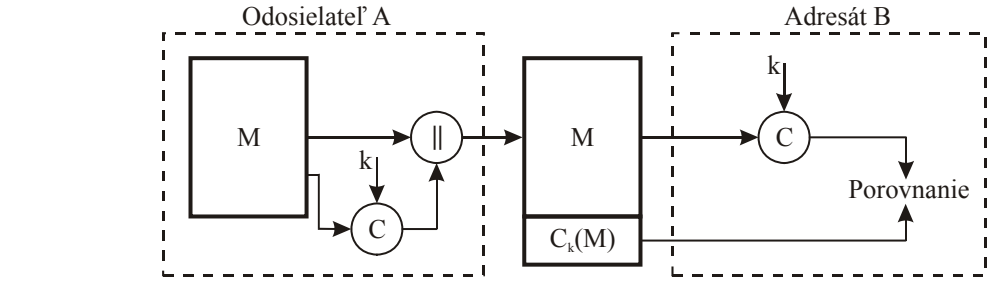


a.

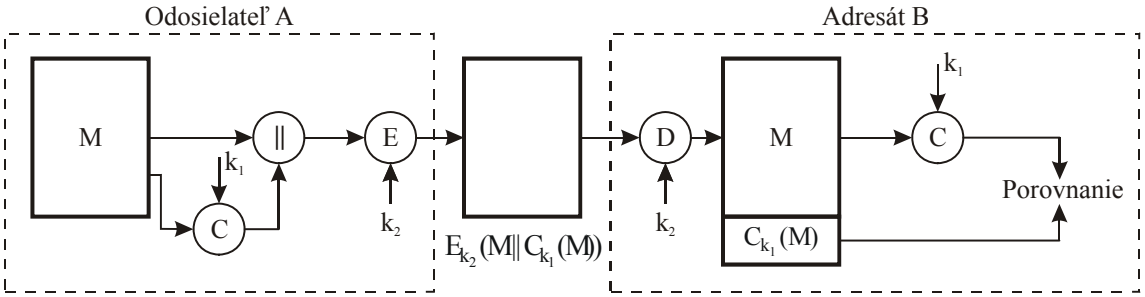


b.

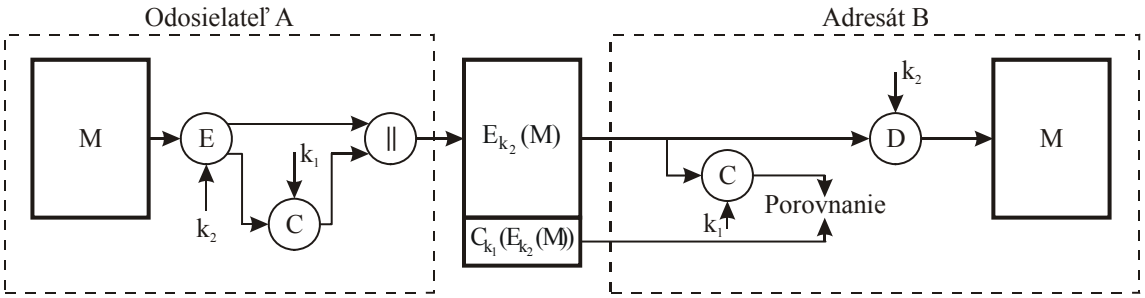
Obr. 9.2 Kryptografický kontrolný súčet, a - interný, b - externý



a)



b)



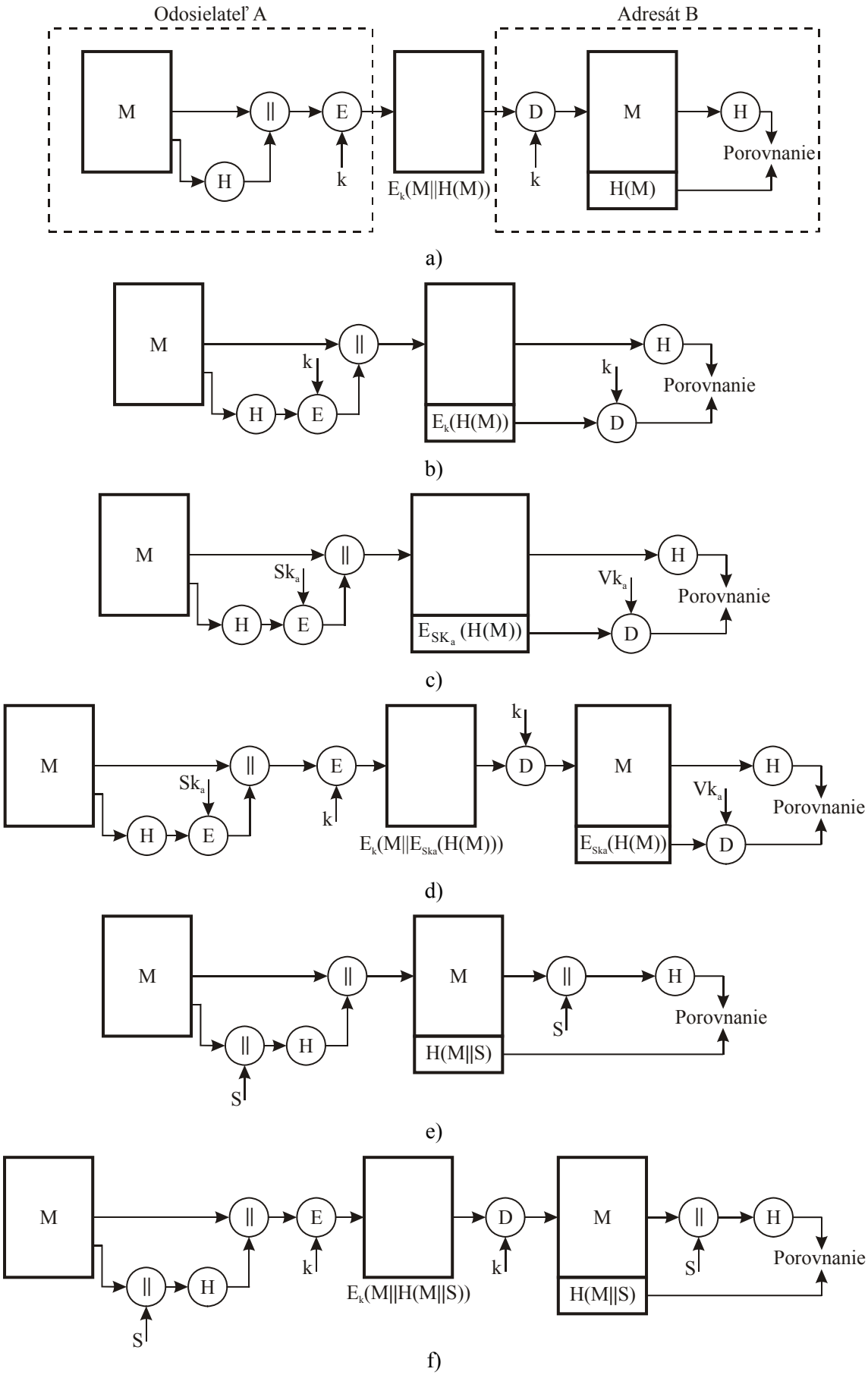
c)

Obr. 9.3 Použitie funkcie MAC

a) Autentizácia správy

b) Utajenie a autentizácia správy pripojená k otvorenému textu

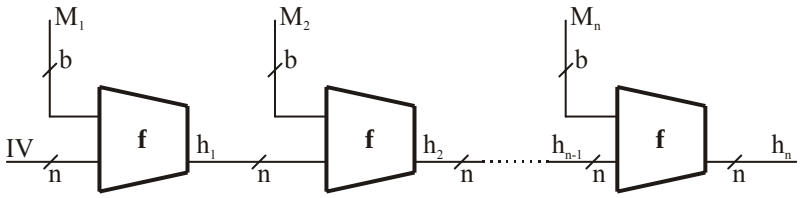
c) Utajenie a autentizácia správy pripojená k zašifrovanému textu



Obr. 9.4 základné spôsoby použitia hašovacích funkcií

	bit 1	bit 2	bit 3	. . .	bit *n*
Blok 1	b_{11}	b_{21}	b_{31}	. . .	b_{n1}
Blok 2	b_{12}	b_{22}	b_{32}	. . .	b_{n2}
Blok 3	b_{13}	b_{23}	b_{33}	. . .	b_{n3}
	⋮	⋮	⋮	⋮	⋮
Blok *m*	b_{1m}	b_{2m}	b_{3m}	. . .	b_{nm}
Hašovací kód *h*	h_1	h_2	h_3	. . .	h_n

Obr. 9.5 Jednoduchá hašovacia funkcia s využitím operácie XOR



Obr. 9.6 Štruktúra iteračných hašovacích funkcií