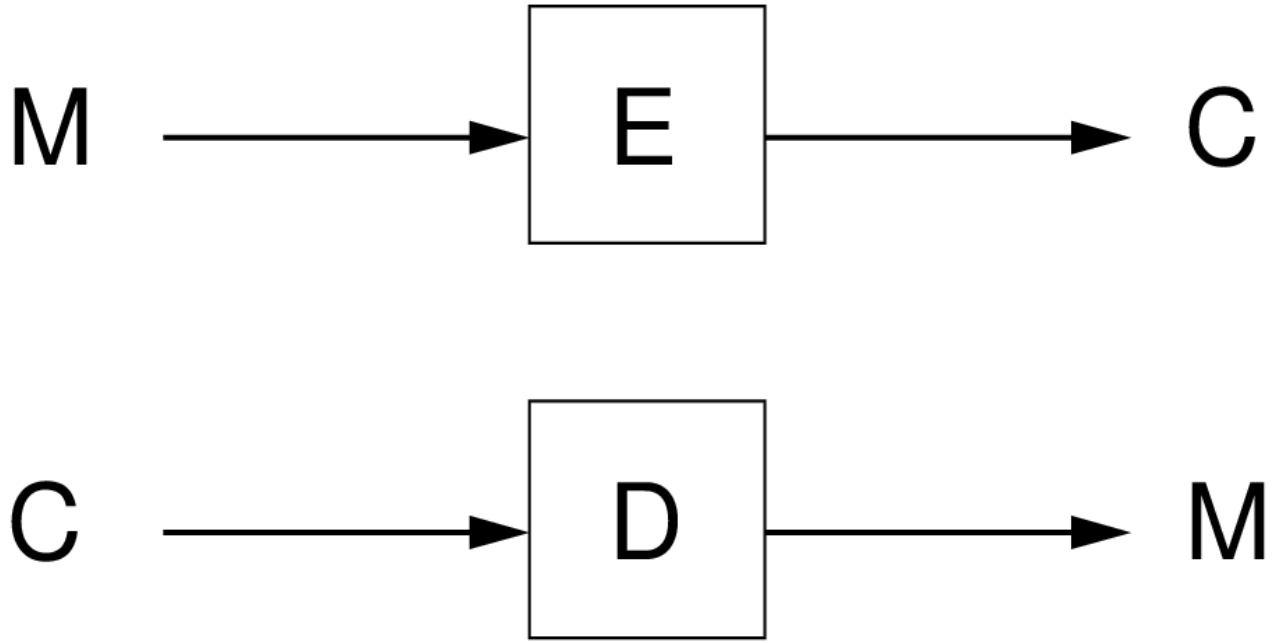
Elektronický podpis

Úvod do problematiky

Informační politika

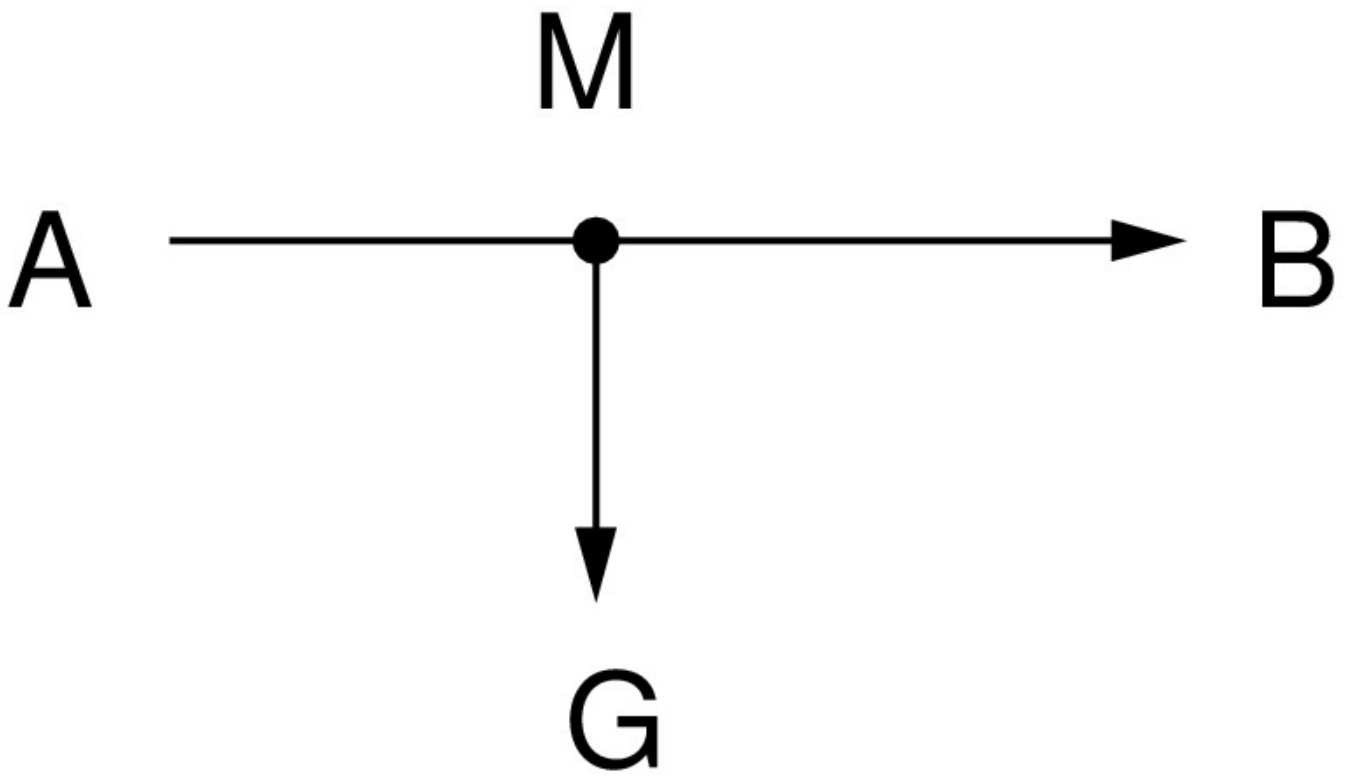
9. 11. 2012

Kryptografie



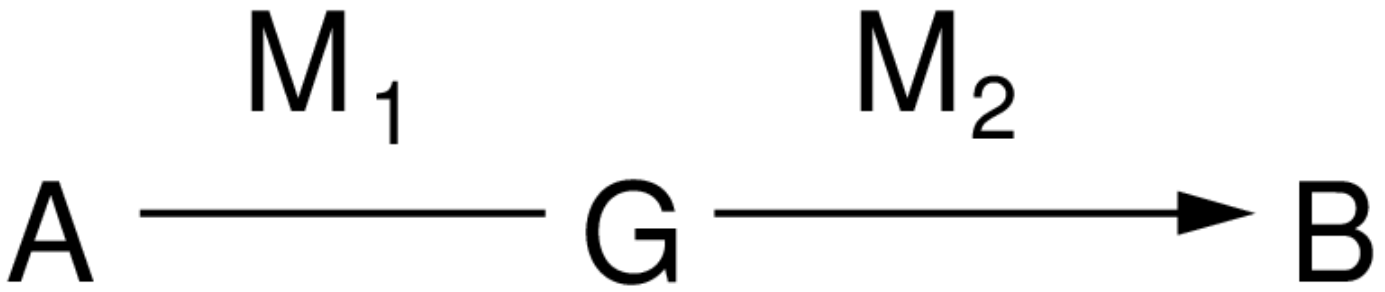
Encryption – šifrování
Message – zpráva
Decryption – dešifrování
Cryptotext – šifrovaná zpráva

Důvěrnost (utajení)



M: Bobe, nikomu to neříkej, ale Gita je hloupá.

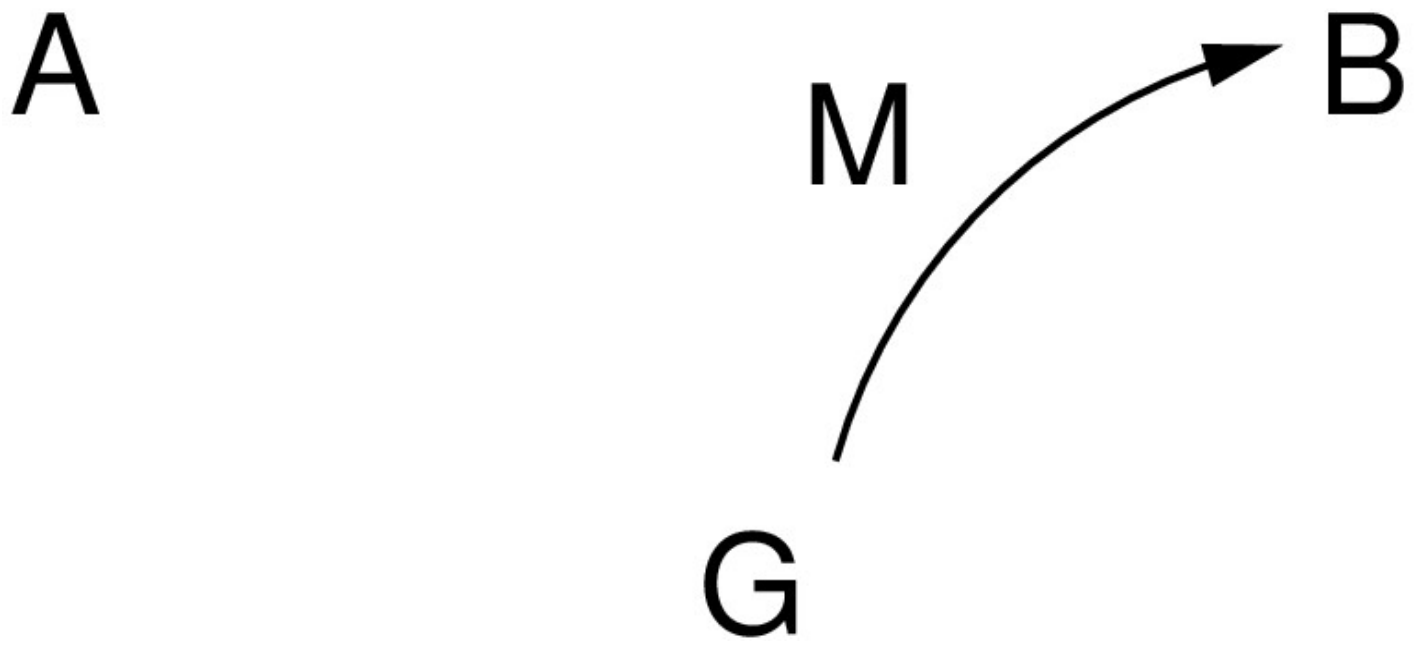
Integrita



M_1: Bobe, miluji tě.

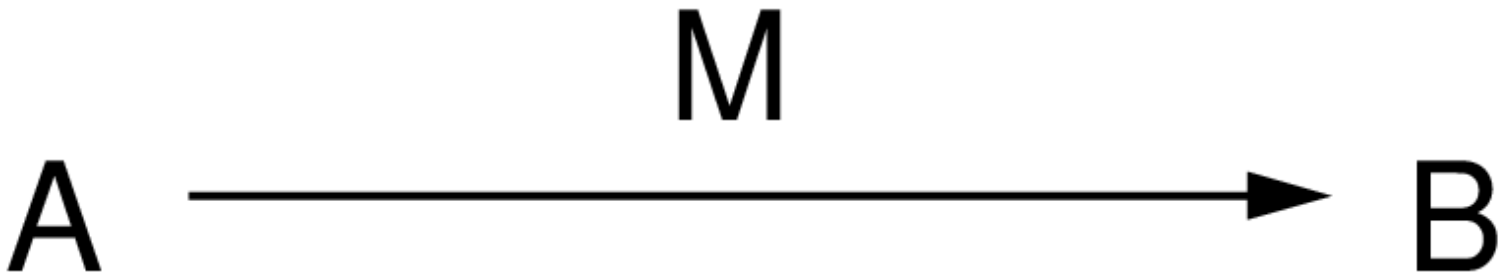
M_2: Bobe, nenávidím tě.

Autenticita



M: Bobe, přijď dnes v 5 do hospody, Alice.

Nepopiratelnost

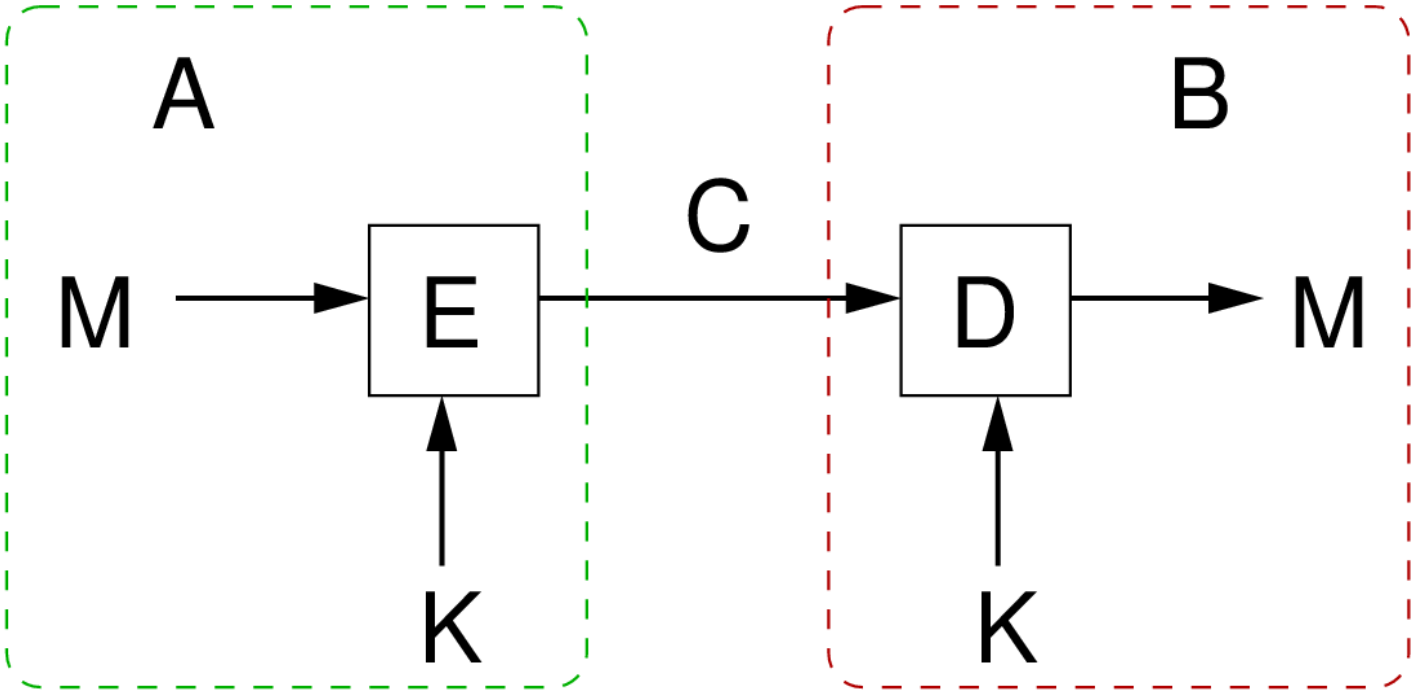


M: Bobe, dej mi milion, nebo to zveřejním.

A: Já to nenapsala!

B: Já jsem si to nevymyslel.

Symetrická kryptografie



M = message: zpráva
K = key: **tajný klíč**
E = encryption: zašifrování

C = cryptotext: zašifrovaná zpráva
D = decryption: dešifrování

Symetrická kryptografie

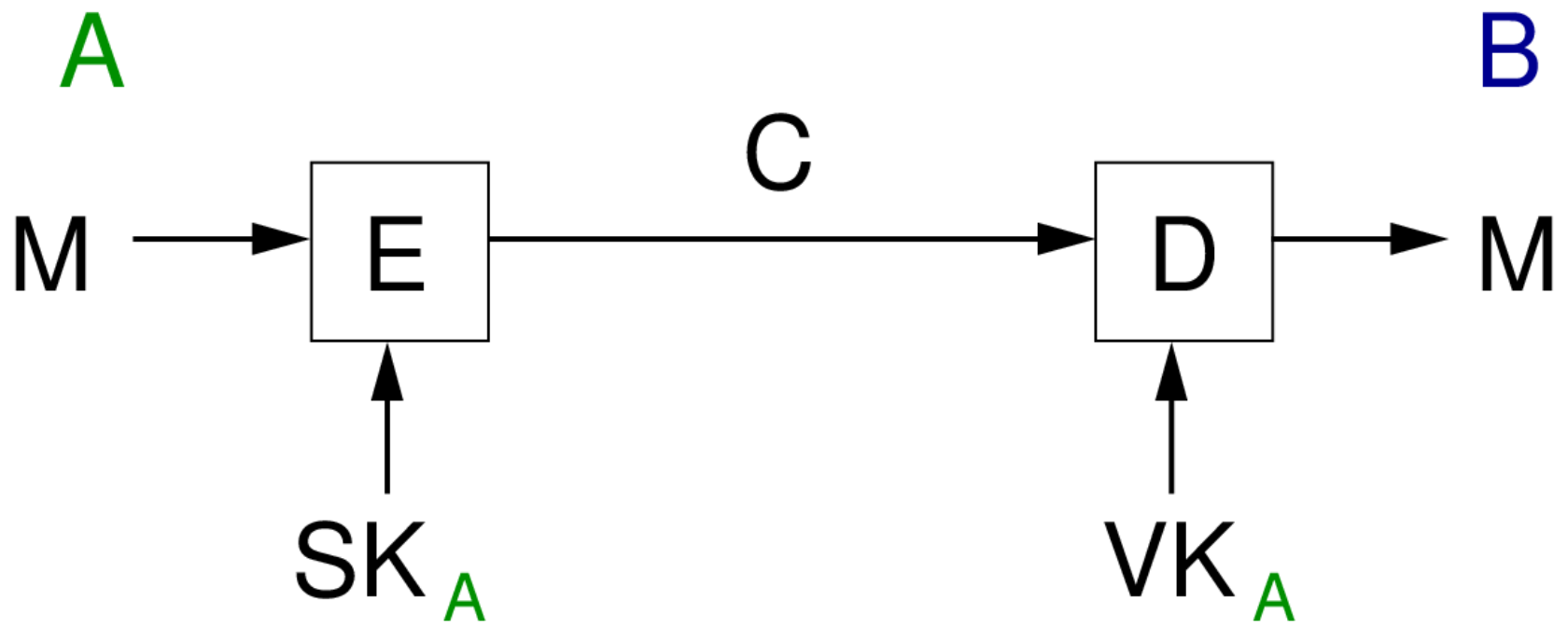
G ?

důvěrnost integrita

autenticita ~~nepopiratelnost~~

Asymetrická kryptografie

(soukromým klíčem)

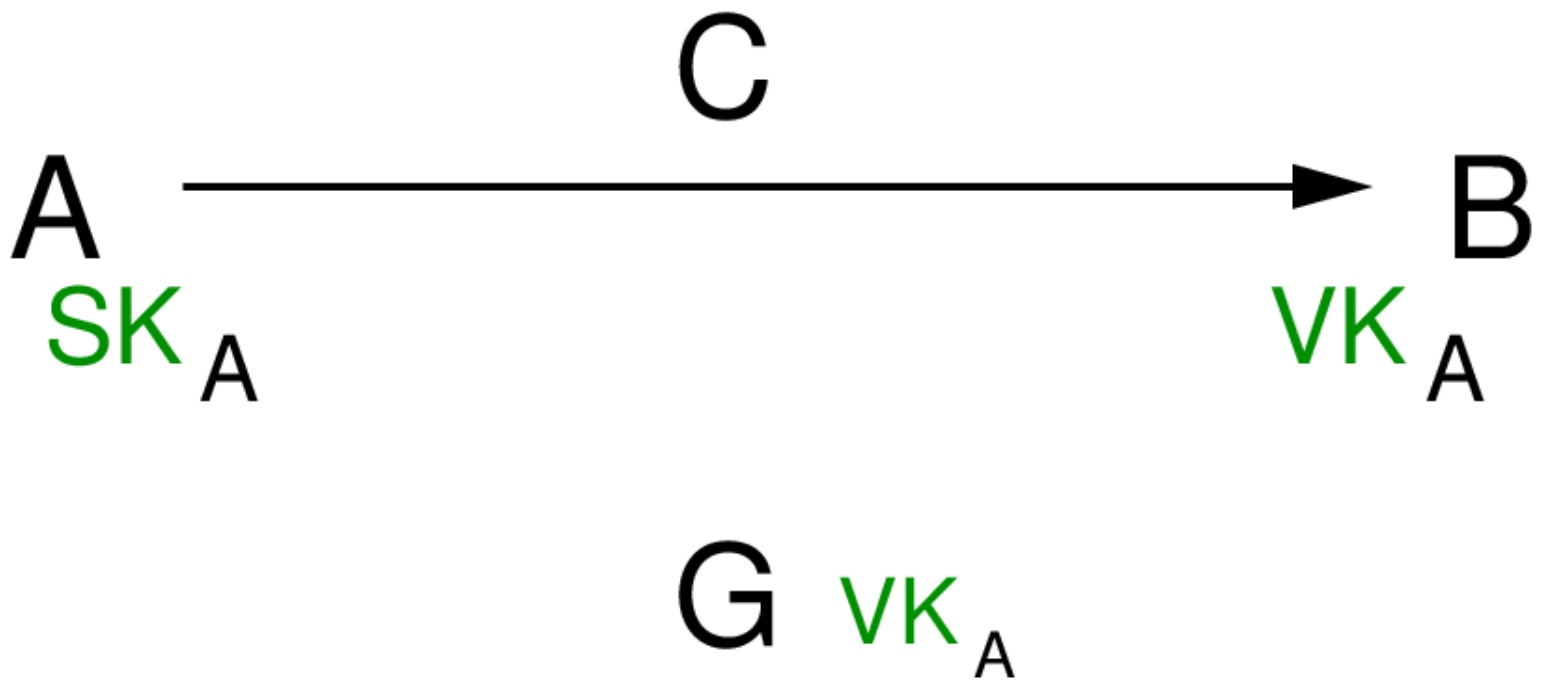


SK_A – soukromý (**tajný**) klíč Alice

VK_A – veřejný klíč Alice

Asymetrická kryptografie

(soukromým klíčem)



~~důvěrnost~~ integrita

autenticita **nepopiratelnost**

Hashovací funkce

Zpráva – dlouhá posloupnost Bytů => zašifrovat ji asymetrickou kryptografií je výpočetně náročné

Hashovací funkce (h)

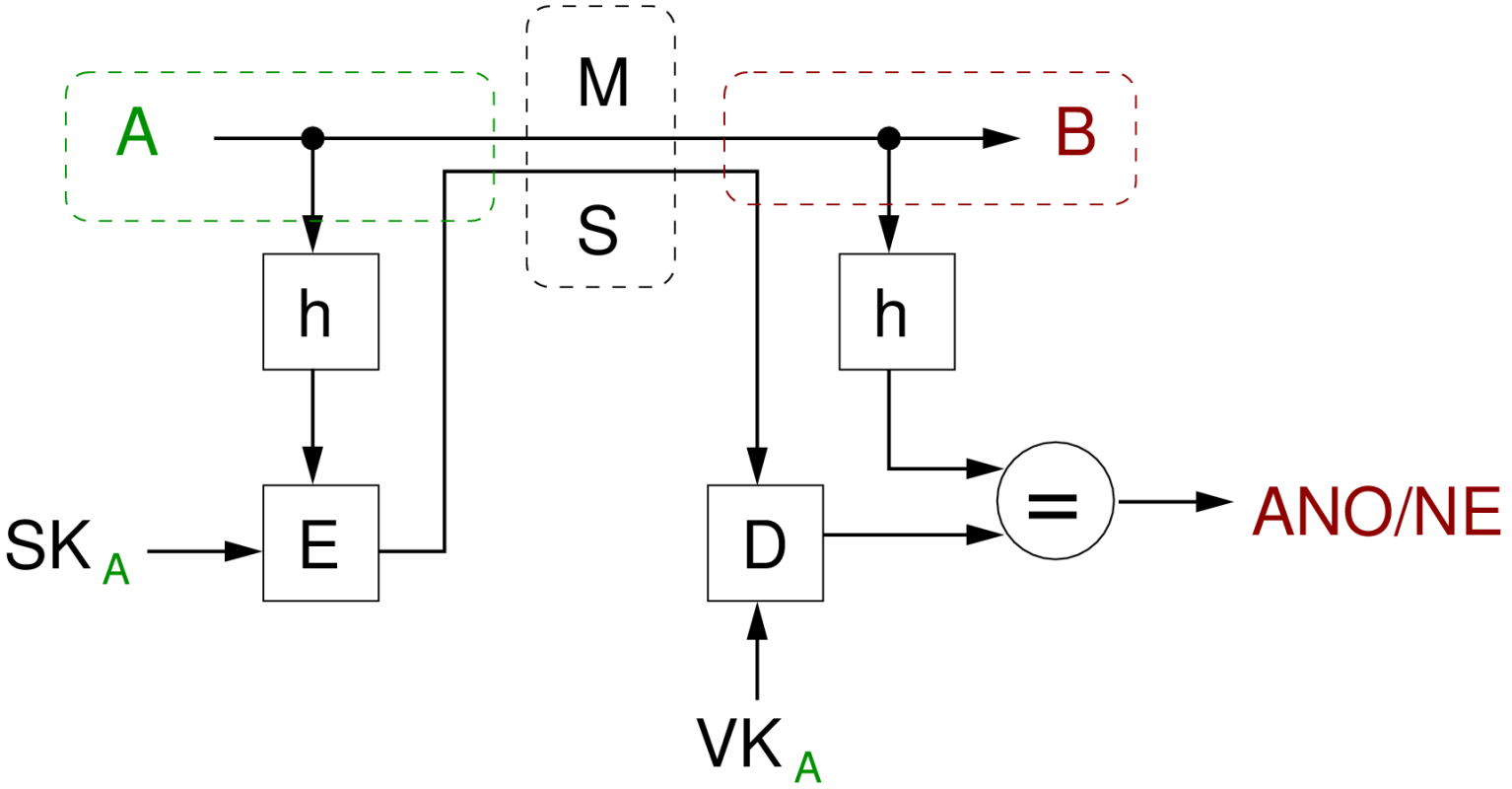
- vstup: libovolně dlouhá posloupnost Bytů
- výstup: fixní posloupnost Bytů = hash (otisk)
- jednocestná a bezkolizní

Elektronický podpis

- Zákon 227/2000 Sb. o elektronickém podpisu:

„údaje v elektronické podobě připojené k datové zprávě, slouží jako metoda k ověření identity podepsané osoby“

Elektronický podpis



Posílá se zároveň M a S (Signature – Podpis).
Bob ověřuje, zda S odpovídá M.

Děkuji za pozornost.