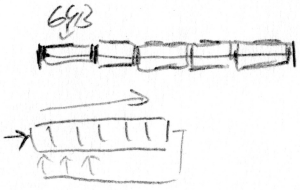
PŘ 9/11

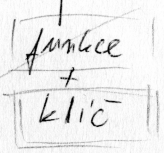
Šifrování a bezpečnost

- Simon Singh: kniha o šifrách

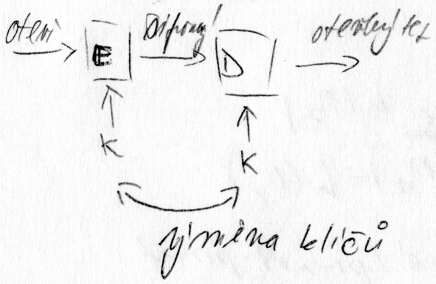
Typy šifer
- symetrické
  - blokové
  - proudové
- asymetrické



šifrování = otevřený text → šifrovaný text

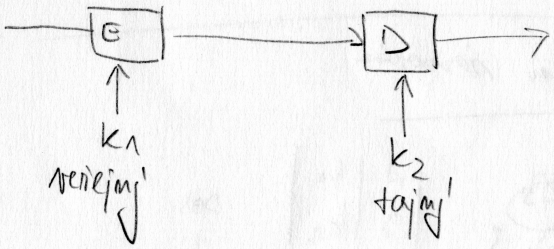


Symetrické



výměna klíčů

Asymetrické



sym. < substituce A ⇒ +
transpozice AHOJ ⇒ JHOA

Složené šifry

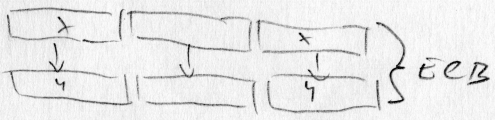
- DES + TRANSP
- Feistelova síť

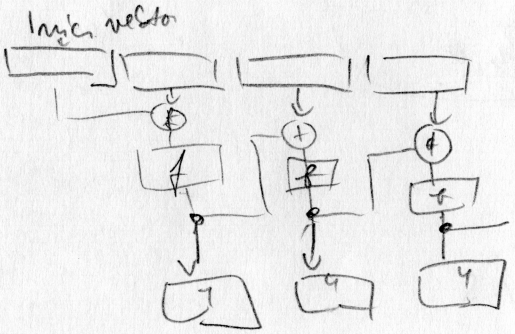
Jednoduché heslo

$(A \oplus k) \rightarrow B \oplus k \rightarrow A$

- XOR

DES





CBC
Change block cipher
= řetězené šifrování

Výměna klíčů

Diffie-Hellman

prvočíslo N
g
x

$X = (g^x) \bmod N$

g, N, X →

$y =$
$Y = (g^y) \bmod N$

←

$X^Y = Y^X = k^Y$

DOK

PE912

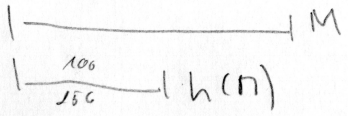
RSA

p, q ... prvočísla

$k_{1,2}$ k^+ ... veřejný klíč

k^- ... tajný klíč

Hashovací fce



MD A
SHA-1

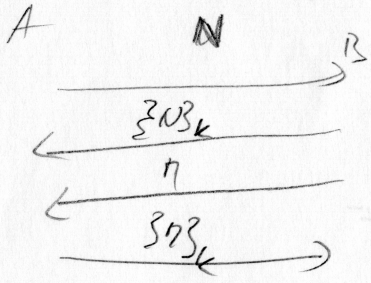
⇒ zjednodušeně

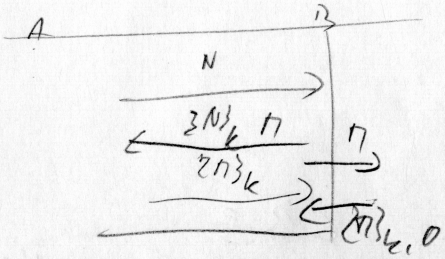
m_1 $h(m_1) \xrightarrow{?} m_2$ $h(m_2)$

$h(m_1) = h(m_2)$

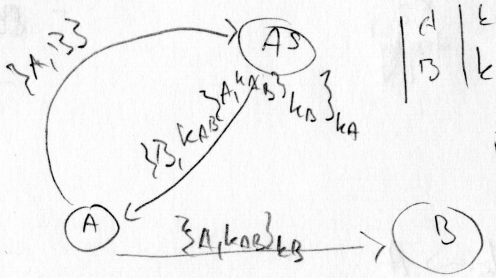
OVĚŘOVÁNÍ

- vzájemné (přímé) - přímé
- nepřímé (obsahuje rozhodčí)
  - symetrické
  - nesymetrické





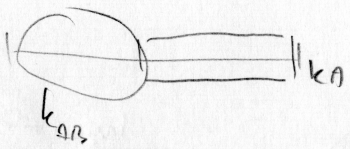
Obecné ověřovací schéma



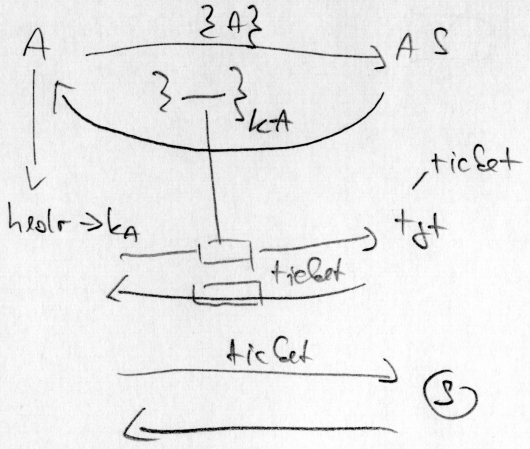
A	k_A
B	k_B

DES

heslo → klíč

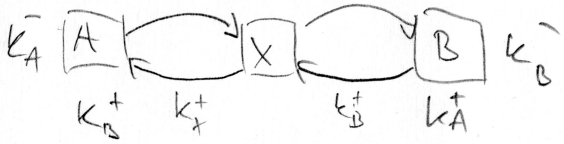


KERBEROS



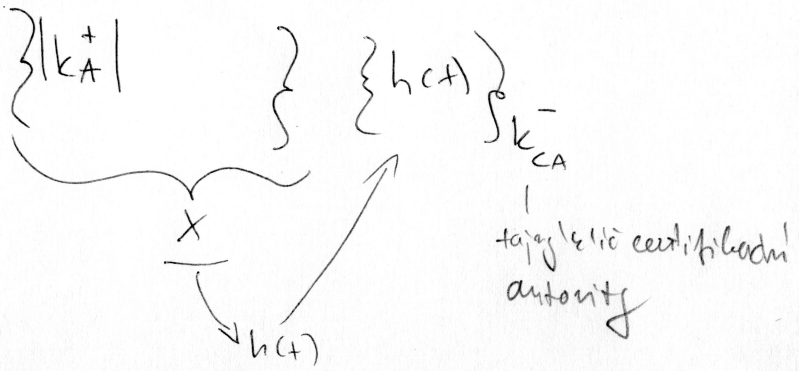
Obětovaný - nevěrný klíč

Man in the middle



certifikát

Obahuje také nevěrný klíč!



29/3