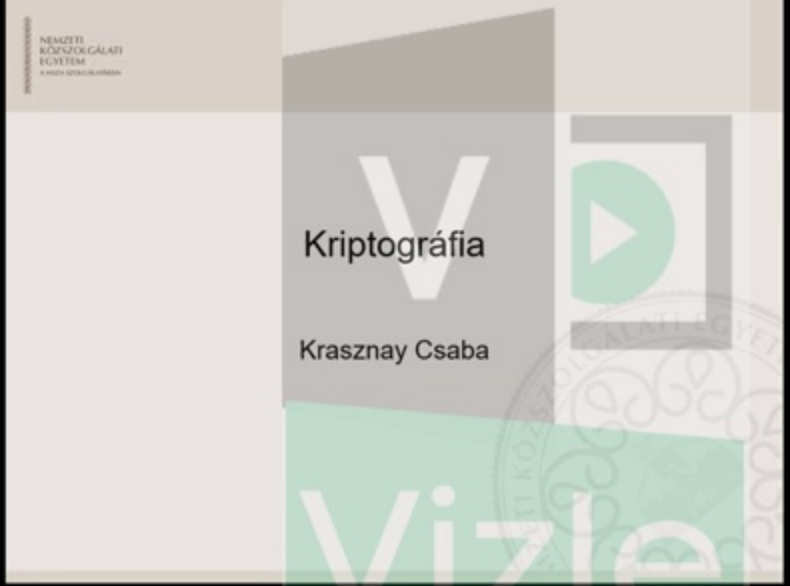
NEMZETI
KÖZSZOLGÁLATI
EGYETEM
Kriptográfia
Krasznay Csaba

https://vizle.offnote.co

Contact us: **vizle@offnote.co**

This document was generated automatically by **Vizle**

Your **Personal Video Reader Assistant**

Learn from Videos **Faster** and **Smarter**

VIZLE **PRO / BIZ**

PDF, PPT ~~Watermarks~~

- Convert *entire* videos
- *Customize* to retain all essential content
- Include Spoken *Transcripts*
- Customer support

Visit **https://vizle.offnote.co/pricing** to learn more

VIZLE **FREE PLAN**

PDF only Watermarks

- Convert videos *partially*
- Slides may be *skipped**
- Usage restrictions
- No Customer support

Visit **https://vizle.offnote.co** to try free

Login to Vizle to unlock more slides*

A Kerkhoff elv

- Auguste Kerckhoff (holland kriptográfus, 1835-1903): „A titkosítási rendszer megbízhatósága nem alapulhat az algoritmus titokban tartásán, csak a kulcsok titkosságán”
- Shannon: „Az ellenség ismeri a rendszert.”
- Schneier: „A titkosítási rendszerben azt kell titokban tartani, amit a legkönnyebben tudunk cserélni, ha ismertté válik.”
- A „security by obscurity” általában bukás

Még történelem

- 1991: Phil Zimmermann – PGP
- 1994: RC5
- 2000: AES (Rijndael)

Példák

- Szimmetrikus
  - DES
  - double, triple-DES
  - IDEA
  - RC5
  - AES (Rinjdael)
- Nyílt kulcsú
  - RSA
  - ElGamal
  - Diffie-Hellman
  - Elliptikus Görbék
- Hash
  - SHA-256
  - SHA-1
  - MD5

Date	Minimum of Strength	Symmetric Algorithm	Factoring Modulus	Discrete Logarithm Key Group	Elliptic Curve	Hash (A)	Hash (B)
(Legacy)	80	2TDEA*	1024	160	1024	160	SHA-1**	
2016 - 2030	112	3TDEA	2048	224	2048	224	SHA-224 SHA-512/224 SHA3-224	
2016 - 2030 & beyond	128	AES-128	3072	256	3072	256	SHA-256 SHA-512/256 SHA3-256	SHA-1
2016 - 2030 & beyond	192	AES-192	7680	384	7680	384	SHA-384 SHA3-384	SHA-224 SHA-512/224
2016 - 2030 & beyond	256	AES-256	15360	512	15360	512	SHA-512 SHA3-512	SHA-256 SHA-512/256 SHA-384 SHA-512 SHA3-512

Alkalmazások

- Tárolt adatok titkosítása,
- Azonosítás és hitelesítés (pl. TLS, Kerberos),
- Hálózati kommunikáció titkosítása (pl. SSL, VPN),
- Dokumentumok sértetlenségének biztosítása,
- Operációs rendszer sértetlenségének biztosítása, stb.
- Nyílt kulcsú infrastruktúra (Public Key Infrastructure – PKI)

https://vizle.offnote.co

Contact us: **vizle@offnote.co**

This document was generated automatically by **Vizle**

Your **Personal Video Reader Assistant**

Learn from Videos **Faster** and **Smarter**

VIZLE **PRO / BIZ**

PDF, PPT ~~Watermarks~~

- Convert *entire* videos
- *Customize* to retain all essential content
- Include Spoken *Transcripts*
- Customer support

Visit **https://vizle.offnote.co/pricing** to learn more

VIZLE **FREE PLAN**

PDF only Watermarks

- Convert videos *partially*
- Slides may be *skipped**
- Usage restrictions
- No Customer support

Visit **https://vizle.offnote.co** to try free

Login to Vizle to unlock more slides*