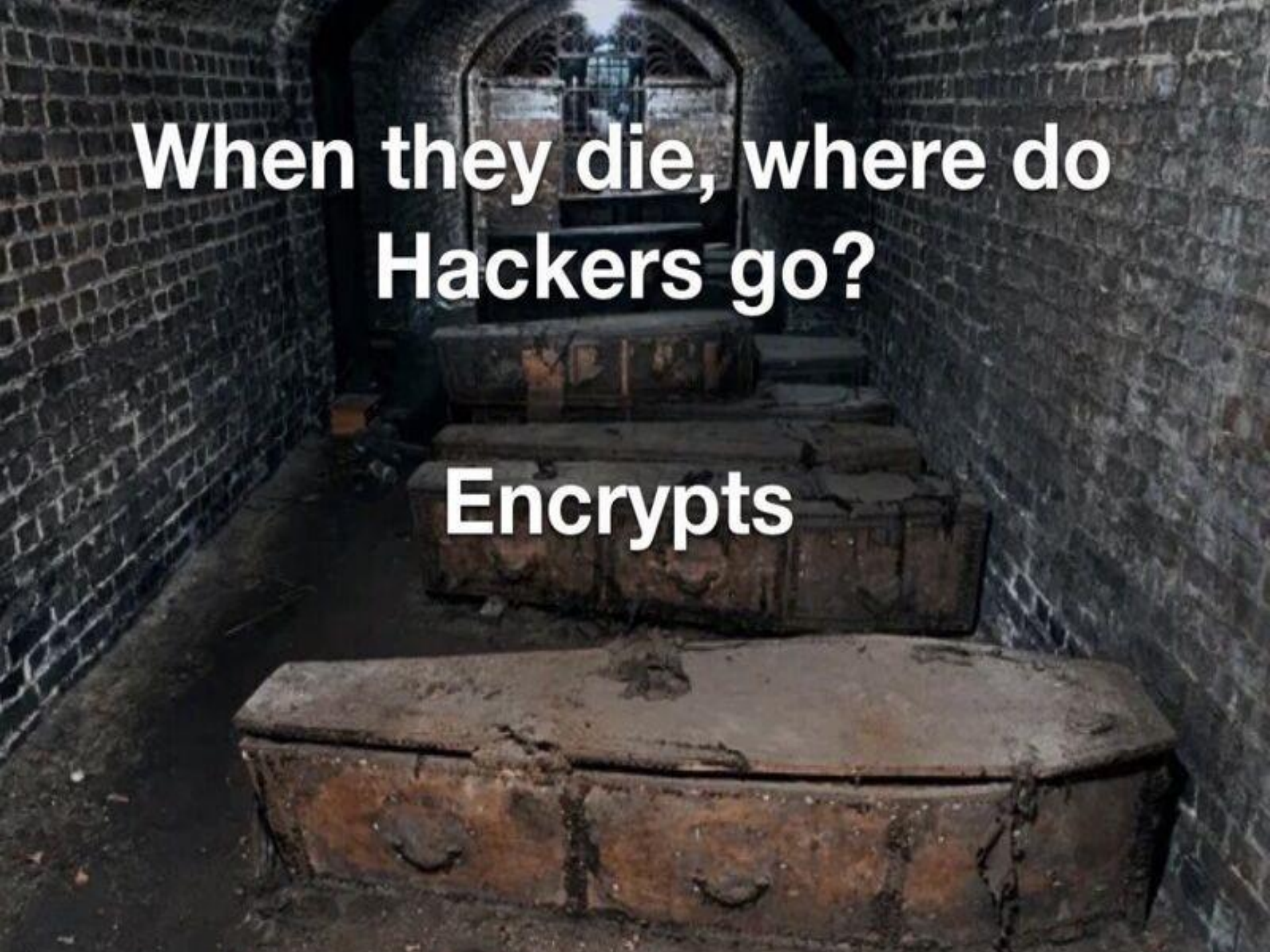

When they die, where do Hackers go?
Encrypts

Standardizace v oblasti kryptografie

Motto: Pokud chcete něco chránit, naučte se to nejprve rozbít …

Jan Dušátko
Únor 2022

Dávná historie?

- První standardizace kryptografie mezi římskými legiemi (Caesarova šifra ROT13)
- Metoda kódování do pětic znaků převzata od telegramů (průměrná délka slov kvůli účtování)
- Rozvoj národních šifrovacích standardů v době I sv. války:

- Plný nástup lokálních standardů v době okolo II sv. války:
  Enigma, Lorenz, Hagelin, Sigaba, C-38, M-2029, SG-41 …
- První celosvětově známý standard DES
- První celosvětově známý standard na základě otevřené soutěže AES
- Druhý celosvětově známý standard na základě otevřené soutěže SHA3

Kerckhoffsovy zákony

1. Systém by měl být prakticky nenapadnutelný, v ideálním případě ho nesmí být možné ohrozit ani teoreticky. *V současnosti to znamená mít matematický důkaz správnosti.*

2. Návrh systému nesmí vyžadovat utajení tohoto návrhu. Případný únik architektury tak neohrožuje bezpečnost komunikace. *Tento princip je používán jako Kerckhoffsův princip.*

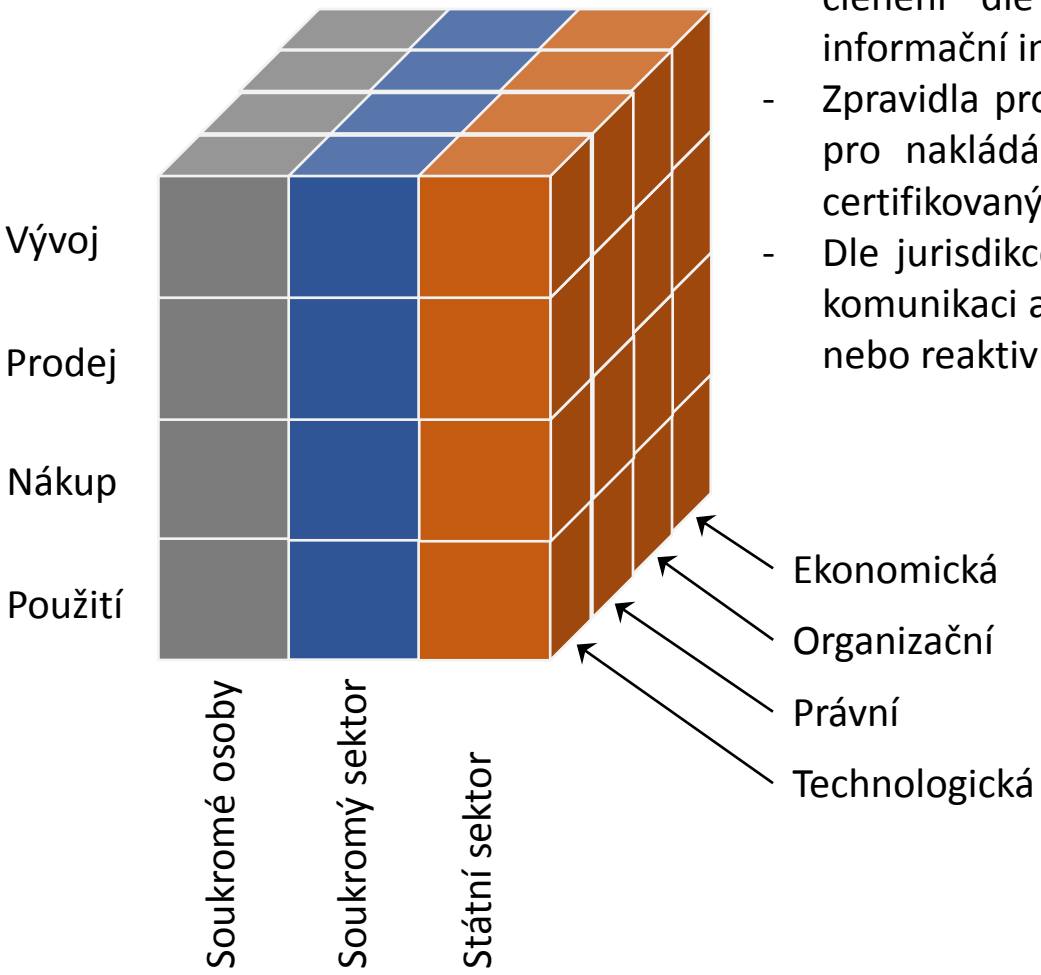
3. Klíč by měl být jednoduše zapamatovatelný, nejlépe bez poznámek, a měl by být snadno měnitelný.

4. Kryptogramy by měly být vysílány telegrafem.

5. Přístroje nebo dokumenty by měly být přenosné a obsluhované jednou osobou.

6. Systém by měl být jednoduchý, nesmí vyžadovat složitá pravidla nebo intelektuální zátěž.

Standardizace kryptografie

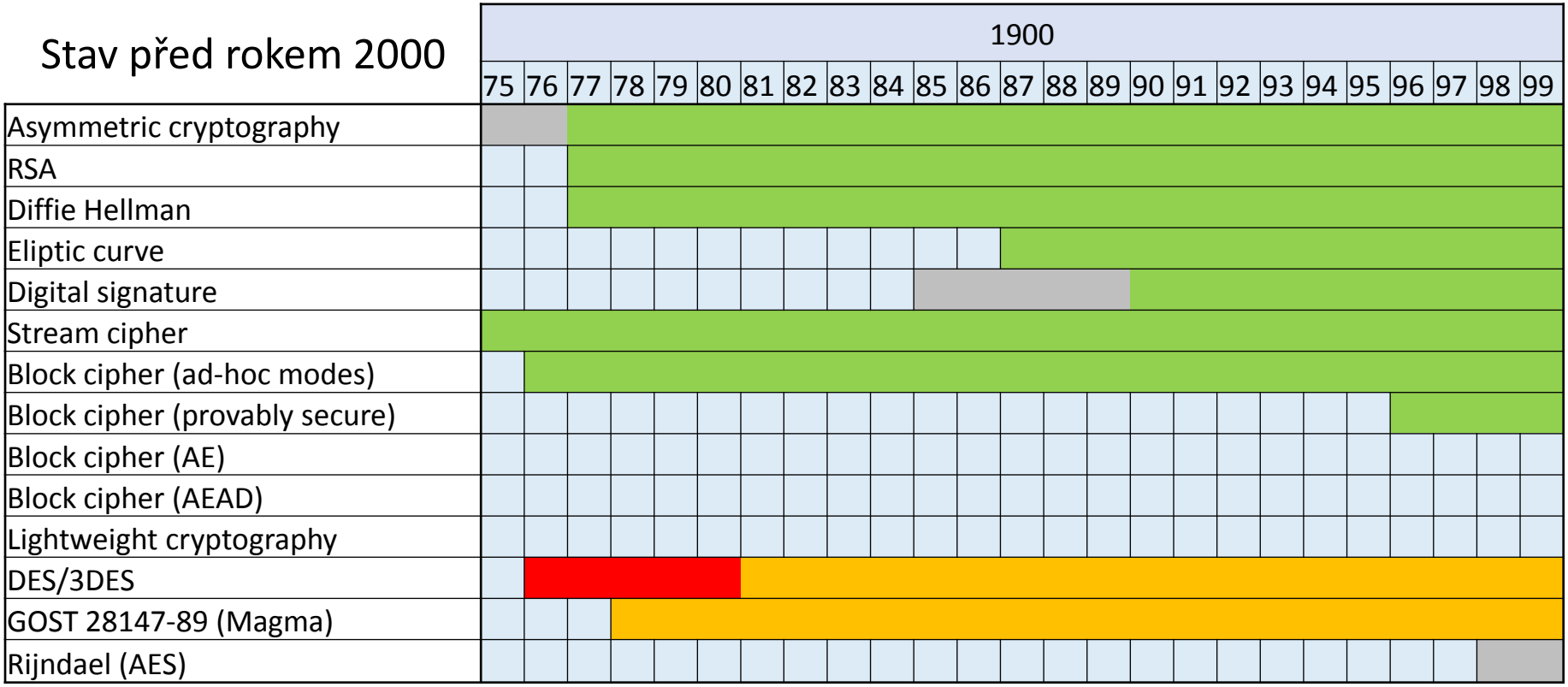


Další, neuvedené rozměry:

- U soukromého a státního sektoru má dále význam členění dle určení systému jako součásti kritické informační infrastruktury.
- Zpravidla pro státní sektor je nutné dodržovat pravidla pro nakládání s utajovanými skutečnostmi a použití certifikovaných systémů.
- Dle jurisdikce pak povinnost vydávání klíčů, záznam o komunikaci a dalších informací, nutných pro preventivní nebo reaktivní omezení.

Symetricky asymetrický úvod

Stav před rokem 2000



Symetrické problémy

DES	64 bit blok /	56 bit klíč	Propustnost o 30% méně než AES	Slabé klíče, komplementární klíče, bruteforce od 1998, Sweet32
3DES	64 bit blok /	112/168 bit klíč	Propustnost 3x menší než DES	Sweet32
Magma	64 bit blok /	256 bit klíč	Propustnost 3x vyšší než DES	Slabé klíče, Sweet32
RC4	proudová	40-2048 bit klíč	Propustnost 10x vyšší než DES	RC4 bias, Bar Mitzvah, NOMORE ….

První kryptoválka a její dopady

Vývoj:

- PGP (Pretty God Privacy)
- Vytvořeno Philem Zimmermanem v roce 1991
- Bez oprávnění byl použit patentovaný algoritmus RSA, to vedlo k soudnímu sporu
- V roce 1995 vydal knihu „PGP Source Code and Internals“ aby obešel exportní omezení
- Soudní spor se změnil z neoprávněného použití patentu na boj o právo na svobodu projevu
- V roce 1996 byl soudní spor ukončen

Interpretace:

- Protože kryptografie brána jako ekvivalent zbraní, jedná se zároveň o vyjádření svobody projevu a právo držet zbraň
- Každý má právo na použití silné kryptografie.
- Umožnil používání silné kryptografie pro internetovou komunikaci (SSL/TLS, IPSec, SSH …)

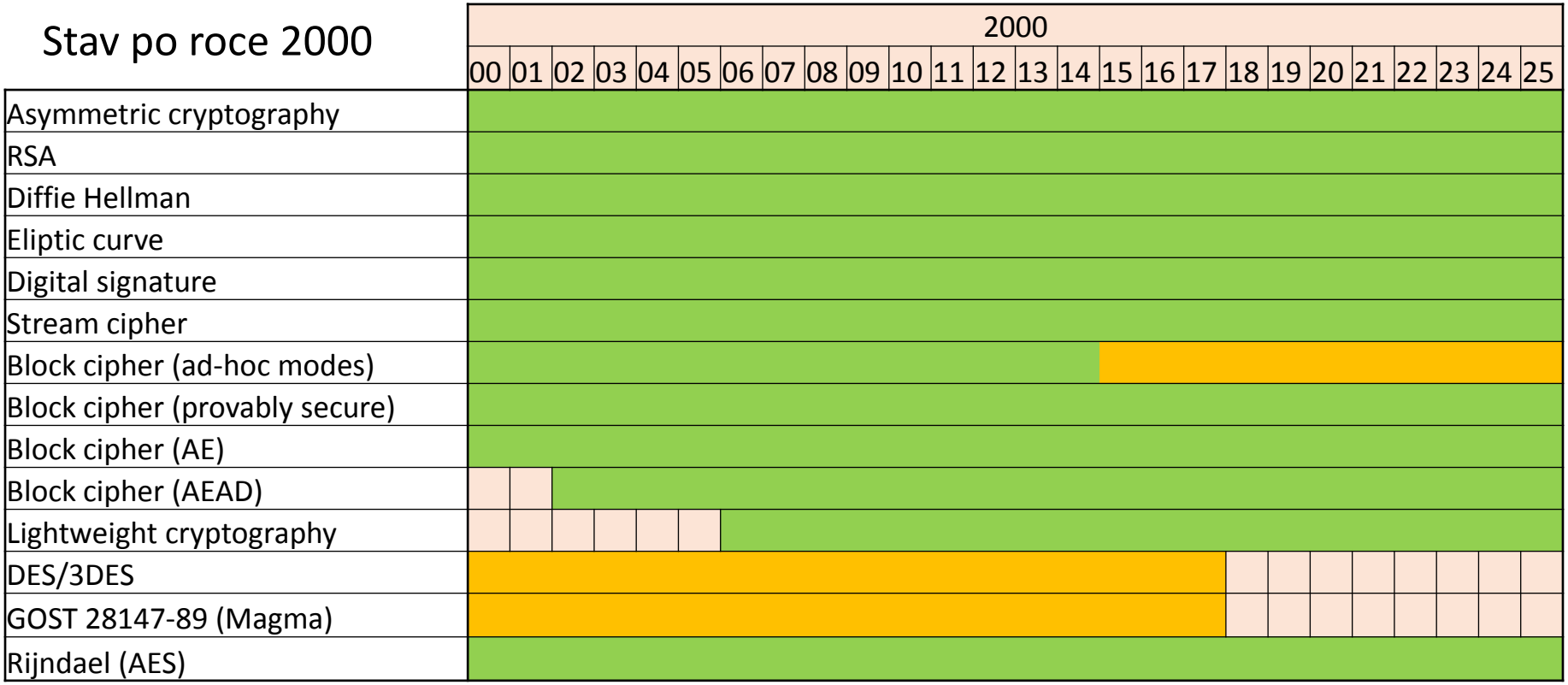
Důsledkem je ztráta monopolu USA na kryptografické algoritmy ve světě IT a snaha chránit důvěrnou komunikaci nestátních subjektů adekvátním způsobem. To byl jeden z pilířů rozvoje IT.

1956 – 1994 CoCom (Coordinating Committee for Multilateral Export Controls)
1996 – Wassenaar Arragnement

You can’t spell „Cryptography“ without „cry“

Symetricky asymetrický úvod 2000+

Stav po roce 2000

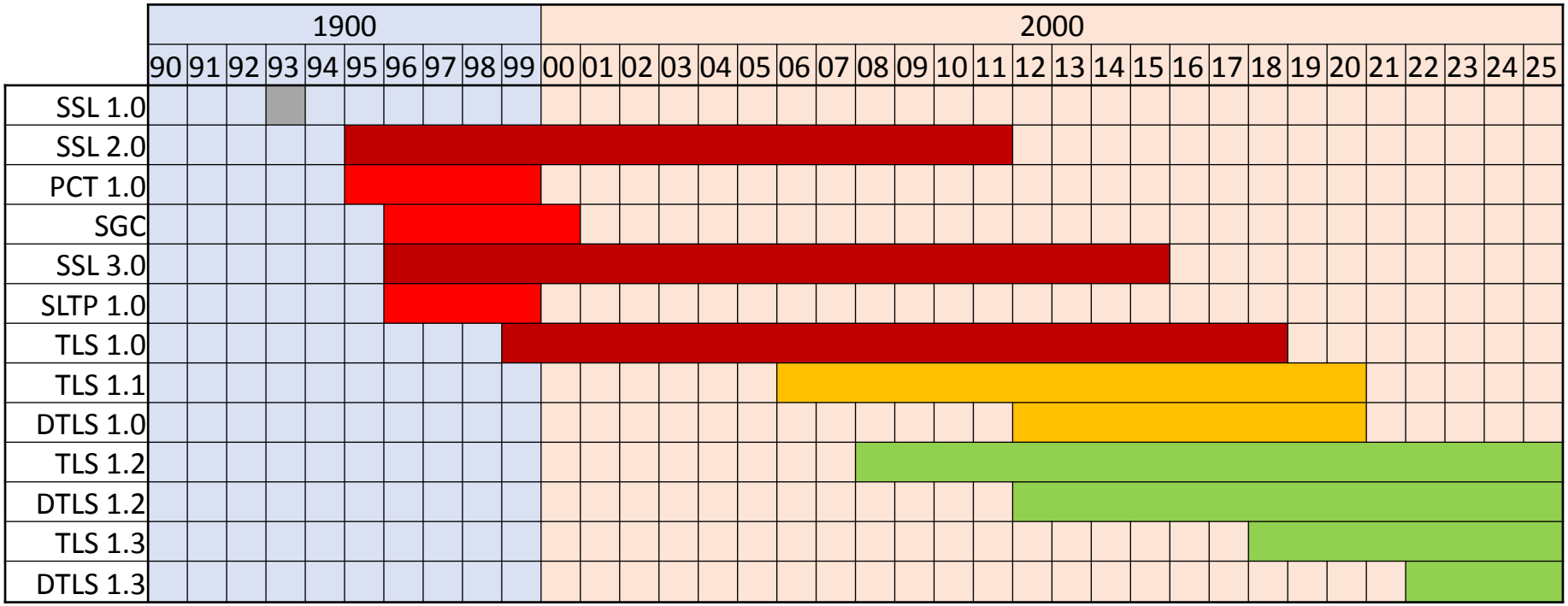


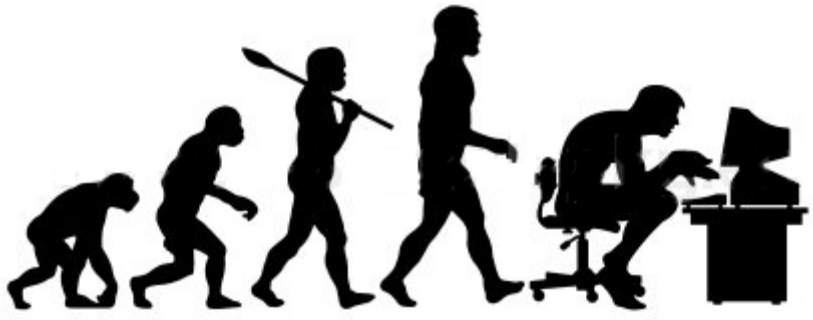
Módy 1 generace obecně nejsou odolné proti změně šifrového textu (proto AE / AEAD módy)

ECB Nedostatek difůze - prosakování vzoru dat
OFB Nepředvídatelná slabina v tvorbě proudu klíčů
CBC Bit flipping – změna bitu ciphertextu pro změnu plaintextu
CFB

PCBC
CNT
CNLF
PCBC

Vývoj SSL/TLS





Snaha o otevřené standardy

	1900					2000																								
	95	96	97	98	99	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
AES																															
Cryptrec																															
Nessie																															
eStream																															
SHA-3																															
CAESAR																															
PHC																															
NIST LWC																															
NIST PQC																															

NIST: AES, SHA2, LWC, PQC
Cordis, IST: Nessie
ECRYPT: eSTREAM

Komunita: CAESAR, PHC

AES (NIST), CRYPTREC (Japonsko)

Round One	Round two	Finalist
CAST-256		
CRYPTON		
DEAL		
DFC		
E2		
FROG		
HPC		
LOKI97		
MAGENTA		
MARS	**MARS**	
RC6	**RC6**	
Rijndael	**Rijndael**	**AES**
SAFER+		
Serpent	**SERPENT**	
Twofish	**Twofish**	

	CRYPTREC 2003	CRYPTREC 2013
64-bit	CIPHERUNICORN-E	
	Hierocrypt-L1	
	MISTY1	3DES-EDE (3k)
128-bit	Camellia	Camellia
	CIPHERUNICORN-A	
	Hierocrypt-3	
	SC2000	AES
Stream	MUGI	
	MULTI-S01	
		Kcipher-2
Hash		SHA2-256
		SHA2-384
		SHA2-512

Nessie (EU CORDIS, IST a akademická sféra)

	Phase 1	Phase 2	Finalist
64-bit	CS-Cipher		
	Hierocrypt -L1		
	IDEA	IDEA	
	Khazad	Khazad	
	MISTY1	MISTY1	**MISTY1**
	Nimbus		
128-bit	Anubis		
	Camellia	Camellia	**Camellia**
	Grand Cru		
	Hierocrypt -3		
	Noekeon		
	Q		
	SC2000		
	AES	AES	**AES**
160-bit	SHACAL	SHACAL-1	
		SHACAL-2	**SHACAL-2**
VBL	NUSH (64/128/256)		
	RC6 (128+)	RC6 (128+)	
	SAFER++ (64/128)	SAFER++ (64/128)	
Stream	BMGL	BMGL	
	Leviathan		
	LILI-128		
	SNOW	SNOW	
	SOBER-t16	SOBER-t16	
	SOBERt-32	SOBERt-32	

eSTREAM (ECRYPT)

Phase 1 (SW)	Phase 2 (SW)	Finalist (SW)
ABC		
CryptMT/Fubuki	CryptMT Version 3	
DICING		
DRAGON	Dragon	
F-FCSR		
Frogbit		
HC-256	HC-128, HC-256	**HC-128**
Hermes8		
LEX	LEX-128, LEX-192, LEX-256	
MAG		
Mir-1		
NLS	NLSv2, encryption-only	
Phelix		
Polar Bear		
POMARANCH		
Py		
Rabbit	Rabbit	**Rabbit**
Salsa20	Salsa20	**Salsa20/12**
SOSEMANUK	SOSEMANUK	**SOSEMANUK**
SSS		
TRBDK3 YAEA		
Yamb		

Phase 1 (HW)	Phase 2 (HW)	Finalist (HW)
Achterbahn		
DECIM	DECIM v2, DECIM-128)	
Edon-80	Edon80	
F-FCSR	F-FCSR-H v2, F-FCSR-16	
Grain	Grain v1, Grain-128	**Grain v1**
Hermes8		
LEX		
MAG		
MICKEY	MICKEY 2.0, MICKEY-128 2.0	**MICKEY v2**
MOSQUITO	Moustique	
NLS		
Phelix		
Polar Bear		
POMARANCH	Pomaranch Version 3	
Rabbit		
Salsa20		
SFINKS		
SSS		
TRBDK3 YAEA		
Trivium	Trivium	**Trivium**
TSC-3		
VEST		
WG		
Yamb		
Zk-Crypt		

SHA3 (NIST)

Phase 1	Phase 2	Phase 3	Finalist
Abacus			
ARIRANG			
AURORA			
BLAKE	BLAKE	BLAKE	
Blender			
BLUE MIDNIGHT WISH	BLUE MIDNIGHT WISH		
BOOLE			
CRUNCH			
CubeHash	CubeHash		
DCH			
Dynamic SHA			
Dynamic SHA2			
ECOH			
EDON-R			
ECHO	ECHO		
EnRUPT			
ESSENCE			
FSB			
Fugue			
Grøstl	Grøstl	Grøstl	
Hamsi	Hamsi		
Cheetah			
CHI			
JH	JH	JH	
Keccak	Keccak	Keccak	**SHA-3**
Khichidi-1			

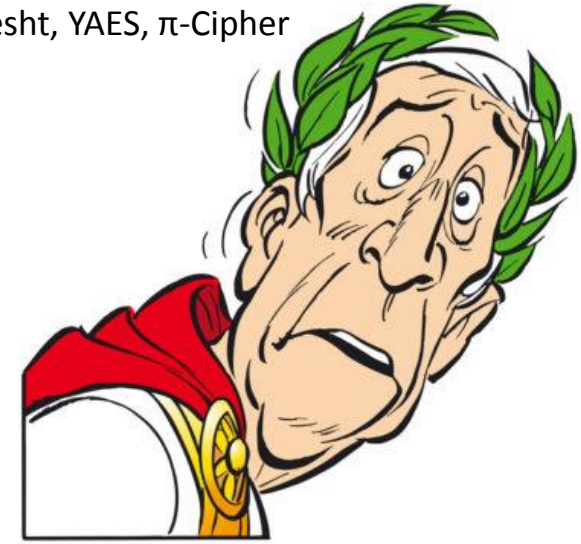
Phase 1	Phase 2	Phase 3	Finalist
LANE			
Lesamnta			
Luffa			
LUX			
MCSSHA-3			
MD6			
MeshHash			
NaSHA			
SANDstorm			
Sarmal			
Sgàil			
Shabal	Shabal		
SHAMATA			
SHAvite-3	SHAvite-3		
SIMD	SIMD		
Skein	Skein	Skein	
Spectral Hash			
StreamHash			
SWIFFTX			
Tangle			
TIB3			
Twister			
Vortex			
WaMM			
Waterfall			

CAESAR (komunita)

List of ciphers

++AE, ACORN, AEGIS-128, AEGIS-256, AES-CMCC, AES-COBRA, AES-CPFB, AES-OTR, AEZ, Artemia, Ascon, AVALANCHE, Calico, CBA, CBEAM, CLOC, COLM, Deoxys-I, Deoxys-II, ELmD, Enchilada, FASER, HKC, HS1-SIV, ICEPOLE, iFeed, iSCREAM, JAMBU, Joltik, Julius, Ketje, Keyak, KIASU, LAC, Marble, McMambo, Minalpher, MORUS, NORX, OCB, OMD, PAEQ, PAES, PANDA, POET, POLAWIS, PRIMATEs-GIBBON, PRIMATEs-HANUMAN, Prøst, Raviyoyla, Sablier, SCREAM, SHELL, SILC, Silver, STRIBOB, Tiaoxin, TriviA-ck, Wheesht, YAES, π-Cipher

First round: 57 algoritmů, 28 odstraněno
Second round: 29 algoritmů přidáno
Third round: 15 algoritmů přidáno



	Lightweight application	High Performance applications	Defense in depth
Finalist	1. Ascon v1.2	1. AEGIS-128 v1.1	1. Deoxys-II v1.0
	2. ACORN v3.0	2. OCB v1.1	2. COLM v1.0
Additional Finalist		3. AEGIS-256	
		4. MORUS v2.0	

Password Hashing Competition (komunita)

Phase 1	Phase 2	Finalist
AntCrypt		
Argon, Argon2	Argon, Argon2	**Argon2**
battcrypt	battcrypt	
Catena	Catena	Catena
Catfish		
Centrifuge		
EARWORM		
Gambit		
Lanarea		
Lyra2	Lyra2	Lyra2
M3lcrypt		
Makwa	Makwa	Makwa

Phase 1	Phase 2	Finalist
MCS_PHS		
Omega Crypt		
Parallel	Parallel	
PolyPassHash		
POMELO	POMELO	
Pufferfish	Pufferfish	
RIG		
Schvrch		
Tortuga		
TwoCats		
Yarn		
yescrypt	yescrypt	yescrypt

Crypt interface (Unix/Linux komunita)

Algorithm	Scheme ID	Scheme	Salt	Round	Description
DES	_	BSDI	3. parametr, 24b	1	Slabé
DES		DES	3. parametr, 12b	25	Slabé
MD5	1	MD5	2. Parametr		Slabé
Blowfish	2	bcrypt	Součást hash[1]	2. Parametr	heslo <72 znaků, zastaralé
Blowfish	$2a$	bcrypt	Součást hash[1]	2. Parametr	heslo <72 znaků CVE-2011-2483
Blowfish	$2b$	bcrypt	Součást hash[1]	2. Parametr	heslo <72 znaků
Blowfish	$2x$	bcrypt	Součást hash[1]	2. Parametr	Heslo <72 znaků
Blowfish	$2y$	bcrypt	Součást hash[1]	2. Parametr	Heslo <72 znaků
MD4	3	NTHASH	Ne	Ne	Slabé
SHA1	4	SHA1	3. Parametr	2. Parametr	Slabé
SHA2	5	SHA-256	3. Parametr	2. Parametr	
SHA2	6	SHA-512	3. Parametr	2. Parametr	
scrypt	7	scrypt		2. Parametr	
MD5	$md5,rounds=x$	Solaris MD5	3. Parametr	2. Parametr	Slabé
SHA1	$sha1$	PBKDF1 with SHA-1	3. Parametr	2. Parametr	Slabé
SHA2	$sha256$	PBKDF2 with SHA-256	3. Parametr	2. Parameter	
SHA2	$sha512$	PBKDF2 with SHA-512	3. parametr	2. Parametr	
ARGON2D	$argon2d$	Argon2	3. Parametr	2. Parametr	
ARGON2I	$argon2i$	Argon2	3. Parametr	2. Parametr	
yescrypt	gy	ghost-yescrypt	3. Parametr	2. Parametr	Streebog S-Box
yescrypt	y	yescrypt	3. Parametr	2. Parametr	

[1]) Sůl je součástí řetězce obsahujícího hash hesla. Jedná se o prvních 22 znaků, poté je bez dalšího rozdělení přiložena hash hesla

LighWeightCryptography (NIST)

List of ciphers

ACE, ASCON, Bleep64, CiliPadi, CLAE, CLX, COMET, DryGASCON, Elephant, ESTATE, FlexAEAD, ForkAE, Fountain, GAGE and InGAGE, GIFT-COFB, Gimli, Grain-128AEAD, HERN & HERON, HYENA, ISAP, KNOT, LAEM, Lilliput-AE, Limdolen, LOTUS-AEAD and LOCUS-AEAD, mixFeed, ORANGE, Oribatida, PHOTON-Beetle, Pyjamask, Qameleon, Quartet, REMUS, Romulus, SAEAES, Saturnin, Shamash & Shamashash, SIMPLE, SIV-Rijndael256, SIV-TEM-PHOTON, SKINNY-AEAD/SKINNY-HASH, SNEIK, SPARKLE (SCHWAEMM and ESCH), SPIX, SpoC, Spook, Subterranean 2.0, SUNDAE-GIFT, Sycon, Thank Goodness It's Friday (TGIF), TinyJambu, Triad, TRIFLE, WAGE, Xoodyak

First round: 57 algoritmů, 56 se zůčastnilo
Second round: 32 algoritmů

Name
ASCON
Elephant
GIFT-COFB
Grain128-AEAD
ISAP
Photon-Beetle
Romulus
Sparkle
TinyJambu
Xoodyak

Očekávaný vliv na:

- IoT technologie
- Nositelná elektronika
- RFID technologie
- Senzory a senzorová pole
- SmartCard
- Smart home/house/cars/cities…
- další

Standardizace v Číně a Rusku

Čína: Algoritmy Shang-Mi

Algorithm	Classified	Architecture	Další informace	Use
SM1/SCB2	**Ano**	Blokový	Blok 128b, klíč 128b	Beidou, VPN
SM2	Ne	Asymetrický	ECC 256b pro použití ECDH a ECDSA	TLS, DTLS, VPN
SM3	Ne	Hash funkce	Vstup < 2^{64}B, výstup 256b, ekvivalent SHA256	Beidou, TLS, DTLS, VPN, WAPI
SM4	Ne	Blokový	Blok 128b, klíč 128b, ekvivalent AES	Beidou, TLS, DTLS, VPN, WAPI
~~**SM5**~~	*Nejsou informace o existenci takového algoritmu*			
~~**SM6**~~	*Nejsou informace o existenci takového algoritmu*			
SM7	**Ano**	Blokový	Blok 64b, klíč 128b	Beidou, Přístupové karty
~~**SM8**~~	*Nejsou informace o existenci takového algoritmu*			
SM9	Ne	Asymetrický	ECC 256b pro ECDH a ECDSA	Beidou
ZUC/Zu Chongzhi	Ne	Proudový	Klíč 128b	4G/5G sítě
SSFF3	**Ano**	Blokový		

Rusko: Standardy GOST (***го****сударственный* ***ст****андарт*)

GOST R 28147-89	Magma (64b blok, 256b klíč)
GOST R 34.12-2015	Kuznyechik (128b blok, 256b klíč)
GOST R 34.11-94	Magma based hash, určeno pro digitální podpis
GOST R 34.11-2012	Streebog hash

Post-Quantum Cryptography (NIST)

Round 1 - 69 algoritmů: BIG QUAKE, BIKE, CFPKM, Classic McEliece, Compact LWE, CRYSTALS-DILITHIUM, CRYSTALS-KYBER, DAGS, Ding Key Exchange, DME, DRS, DualModeMS, Edon-K, EMBLEM and R.EMBLEM, FALCON, FrodoKEM, GeMSS, Giophantus, Gravity-SPHINCS, Guess Again, Gui, HILA5, HiMQ-3, HK17, HQC, KCL (aka OKCN/AKCN/CNKE), KINDI, LAC, LAKE, LEDAkem, LEDApkc, Lepton, LIMA, Lizard, LOCKER, LOTUS, LUOV, McNie, Mersenne-756839, MQDSS, NewHope, NTRUEncrypt, pqNTRUSign, NTRU-HRSS-KEM, NTRU Prime, NTS-KEM, Odd Manhattan, Ouroboros-R, Picnic, Post-quantum RSA-Encryption, Post-quantum RSA-Signature, pqsigRM, QC-MDPC KEM, qTESLA, RaCoSS, Rainbow, Ramstake, RankSign, RLCE-KEM, Round2, RQC, RVB, SABER, SIKE, SPHINCS+, SRTPI, Three Bears, Titanium, WalnutDSA

Round 2 – 26 algoritmů

Round 3 - 16 algoritmů

Key Exchange			Digital Signature		
Název	**Princip**	**Zařazení**	**Název**	**Princip**	**Zařazení**
BIKE	Linear code	Secondary	CRYSTALS-DILITHIUM	Lattices	Primary
Classic McEliece	Linear code	Primary	FALCON	Lattices	Primary
CRYSTALS-KYBER	Lattices	Primary	GeMSS	Multivariety	Secondary
FrodoKEM	Lattices	Secondary	Picnic	Symmetric primitivees	Secondary
HQC	Linear code	Secondary	Rainbow	Multivariety	Primary
NTRU	Lattices	Primary	SPHINCS+	Hash based	Secondary
NTRU-Prime	Lattices	Secondary			
SABER	Lattices	Primary			
SIKE	Isogenies	Secondary			

Kvantové počítače a bezpečnost

	Digital computer		Quantum computer	
RSA/DH 1024	$1{,}07*10^{22}$ dní	$2{,}60*10^{9}$ MW	3,53 dní	8,47 MW
RSA/DH 2048	$1{,}15*10^{31}$ dní	$4{,}90*10^{17}$ MW	7,05 dní	16,92 MW
RSA/DH 3072	$4{,}83*10^{37}$ dní	$2{,}60*10^{24}$ MW	10,58 dní	25,39 MW
ECC 256	$4{,}72*10^{34}$ dní	$1{,}13*10^{38}$ MW	3,16 dní	7,58 MW
ECC 384	$8{,}71*10^{53}$ dní	$2{,}09*10^{57}$ MW	4,74 dní	11,37 MW
ECC 512	$1{,}60*10^{73}$ dní	$3{,}84*10^{76}$ MW	6,32 dní	15,16 MW

Odhady:

~2030 První, rozumně použitelné kvantové počítače (nízká úroveň šumu atd.)

???? Komerčně dostupné stroje, použitelné i pro útoky proti kryptografii

Důsledek:

- Vývoj PQC má zpoždění
- Implementace PQC bude výrazně náročnější na znalosti
- klasická asymetrická kryptografie má i po 40 letech problémy s implementací
- Některé informace vyžadují utajení po dlouhou dobu (10+ let)

Problémy generátorů náhodnosti

	1990																2000																					
	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
ANSI X9.31																																									
Fortuna																																									
Linux DRBG (RC4)																																									
Linux DRBG (ChaCha20)																																									
NIST 800-90A DualEC DRBG																																									
NIST 800-90C CTR DRBG																																									
NIST 800-90C Hash DRBG																																									
NIST 800-90C HMAC DRBG																																									
Microsoft CNG DRBG																																									
Microsoft RNG																																									
Yarrow