

2012

Crypto-World 1/2012

A.	Informace redakce, PF 2012	2
B.	Soutěž 2011 – Kompletní příběh včetně úloh, nápověd a jejich správného řešení	3-29
C.	Soutěž 2011 - Statistika soutěže, úspěšnost, řešitelé	30-31
D.	Soutěž 2011 - Ceny a loga sponzorů	31
E.	Pozvánka na SOOM Hacking & Security konferenci	32
F.	O čem jsme psali v lednu 2000 – 2011	33-34
G.	Závěrečné informace	35

Crypto-World 2/2012

A.	Ceskoslovenské šifry z období 2. světové vojny Diel 10., Šifra „Utility“ (J.Kollár)	2 - 10
B.	Lehká kryptografie a pár slov k hackingu (V.Klíma)	11 - 24
C.	Pozvánka na SCIENCE Cafe v Hradci Králové	25
D.	O čem jsme psali v únoru 2000 – 2011	26 – 27
E.	Závěrečné informace	28

Crypto-World 3-4/2012

A.	Ceskoslovenské šifry z období 2. světové vojny Diel 11., Šifra „Palacký“ (J.Kollár)	2 - 12
B.	Má zmysel používať autokľúč? (J.Kollár)	12 - 17
C.	Slabý generátor náhodných čísel umožňuje faktorizovať RSA moduly (O.Mikle, predmluva P.Vondruška)	18 – 21
D.	Call for Papers - Mikulášská kryptobesídka 2012	22
E.	Problematika infrastruktury veřejných klíčů (PKI), dvoudenní kurz Akademie CZ.NIC (P.Vondruška)	23
F.	O čem jsme psali v březnu 2000 – 2011	24 – 25
G.	Závěrečné informace	26

Crypto-World 5-6/2012

A.	HERMANN POKORNY - "zaslúžilý umelec" v lúštiteľskom odbore vo víre I. svetovej vojny (J.Krajčovič)	2 - 8
B.	Najstaršia zašifrovaná písomná pamiatka v Čechách (J.Krajčovič)	9 – 10
C.	Nízkoriziková kryptografie (V.Klíma)	11 - 13
D.	Společná novela zákona o elektronickém podpisu (účinná od 1.7.2012) (P.Vondruška)	14 – 18
E.	Call for Papers - Mikulášská kryptobesídka 2012	19
F.	O čem jsme psali v květnu a v červnu 2000 – 2011	20 – 24
G.	Závěrečné informace	25

Crypto-World 7-8/2012

A.	Andreas Figl – Nestor rakúskej školy kryptológie	2 – 13
B.	Kryptologické perličky 1 (K.Šklíba)	14 – 24
C.	Z NISTu unikl interní dokument k SHA-3 (V.Klíma)	25 - 30
D.	Kniha Kryptologie, šifrování a tajná písma rozebrána (P.Vondruška)	31
E.	Problematika infrastruktury veřejných klíčů (PKI), kurz Akademie CZ.NIC (P.Vondruška)	32 – 23
F.	ZPRÁVA - Nechcete být odposloucháváni? (L.Stejskalová)	34
G.	O čem jsme psali v létě 2000 – 2011	35 – 37
H.	Závěrečné informace	38

Příloha: dokument, který měl být odeslán pouze do interní skupiny NISTu pro výběr SHA-3
(více informací viz článek V.Klímy)

Crypto-World 9-10/2012

A.	Pointerová šifra a nízkoriziková náhrada AES (V.Klíma)	2 – 8
B.	Kryptografické zabezpečení prodeje lihovin (R.Palovský)	9 – 13
C.	Kryptologické perličky 2 (K.Šklíba)	14 – 20
D.	Záhada kodexu Rohonczi Codex (E. Antal)	21 – 28
E.	Kaspersky Lab uvádí Kaspersky Internet Security 2013	29 - 31
F.	O čem jsme psali v září a říjnu 1999 – 2011	32 – 35
G.	Závěrečné informace	36

Příloha: neoglyfy.pdf , ukázka ze sešitu Batěk A. S.: Neoglyfy I., str. 4 – str. 13
(<http://crypto-world.info/casop14/neoglyfy.pdf>)

Crypto-World 11-12/2012

A.	SHA-3 a lehká kryptografie (V.Klíma)	2 – 11
B.	Raně novověká šifrovaná korespondence ve fondech šlechtických rodinných archivů Státního oblastního archivu v Plzni , část I. (J.Mírka)	12 – 28
C.	Tip na vánoční dárek - Enigma - bitva o kód (P.Vondruška)	29 – 30
D.	Pracovní příležitost (World Startup Project)	31
E.	O čem jsme psali v listopadu a prosinci 1999 – 2011	32 – 35
F.	Závěrečné informace	36

Příloha: Obrazová příloha k článku B (Mírka, J.) <http://crypto-world.info/casop14/cast1.zip>