DELAVNICE IZ KRIPTOGRAFIJE

(občasno vključujejo tudi računalniško varnost ali teorijo kodiranja)

1. 1998 FMF–KRIPTOGRAFIJA (1. delavnica) (6)
2. 1999 FMF–KRIPTOGRAFIJA (2. delavnica) (21)
3. 2000 FRI–KIRV (2'. delavnica) (19)
4. 2002 FRI-KIRV (3. delavnica) (15)
5. 2003 FMF–KITK (4. delavnica) (27)
6. 2004 FRI–KIRV (4'. delavnica) (19)
7. 2006 FRI–KIRV (6. delavnica) (7)
8. 2008 IŠRM–KITK2 (18. delavnica) (12)
9. 2008 FRI–KIRV (19. delavnica) (15)
10. 2009 IŠRM–KITK2 (26. delavnica) (13)
11. 2010 IŠRM–KITK2 (31. delavnica) (12)
12. 2010 FRI–KIRV (3)
13. 2011 IŠRM–KITK2 (6?)
14. 2012 IŠRM–KITK2 (36.-38. delavnica) (45)
15. ???
16. 2017 KIRV (39. delavnica) (14)
17. 2018 KIRV (14)
18. 2019 KIRV (72. delavnica) (8)
19. 2020 KIRV (116. delavnica) (18)
20. 2021 KIRV (??)
21. 2022 KIRV (1)
22. 2023 KIRV (doslej: 169+94?=275?)

FMF–KRIPTOGRAFIJA 1998

1)	BAN	Vladimir	Kvantni računalnik
2)	DOLINAR	Gregor	Reševanje kongruenc in Riemanova hipoteza
3)	Luževič	Peter	Nahrbtniški kriptosistemi in LLL algoritem
4)	POVH	Janez	Generatorji pseudonaključnih števil
5)	ŠEGA	Gregor	Testiranje praštevilskosti in Karmichaelova števil
6)	ŽIBERT	Janez	Simetrični sistem IDEA in linearna analiza

FMF–KRIPTOGRAFIJA 1999

1)	BARBIČ	Jernej	Štetje točk na eliptični krivulji
2)	BRŽAN	Irena	Kartice zdravstvenega zavarovanja
3)	FLAJS	Andrej	Generator naključnih števil
4)	IVANEC	Desider	Kriptografski slovar pojmov
5)	JEREB	Mojca	DNK računanje
6)	KOCAN	Peter	Faktorizacija z eliptičnimi krivuljami
7)	KOMAR	Mojca	Prodaja sistemov za varnost podatkov
8)	KAPŠ	Mateja	Zgodovina kriptografije
9)	MEDVED	Mario	Zaščita naše domače strani
10)	MARKOVČIČ	Maja	Slovenska zakonodaja in kriptografija
11)	MIKLAVIČ	Štefko	Algoritmi za potenciranje
12)	NASTRAN	Vanja	Echelon
13)	NOVAK	Tadej	Psevdonaključna zaporedja bitov
14)	PEČAR	Martin	Vizualna kriptografija
15)	PERKO	Urban	Kleptografija - študij varne kraje informacij
16)	PRAPROTNIK	Matjaž	Zgoščevalna funkcija SHA-1
17)	ŠIJANEC	Tina	NSA in računska moč
18)	TONEJC	Jernej	Izboljšanje množenja za določene tipe EC
19)	TROŠT	Matjaž	Brezžični telefoni
20)	VUK	Miha	CA in standard 509
21)	ZUPAN	Eva	Mehanski stroji za faktorizacijo

FRI–KIRV 2000

1)	BENEDIK	Hubert	Hitro odkrivanje potenc praštevil
2)	CEFERIN	Tomo	Izvoz kriptografske tehnologije, patenti
3)	DOBROVOLJC	Andrej	Microsoft CryptoAPI - Kriptografski programski vmesnik
4)	HRASTOVEC	Marko	Ali je kupovanje preko interneta varno - www.eon.si
5)	KAVŠEK	Branko	
6)	KOLMANIČ	Robert	Stanje v Sloveniji na področju pametnih kartic.
7)	KOTNIK	Samo	Elektronsko bančništvo v sloveniji
8)	LEBEN	Roni	Analiza varnosti sistema GSM
9)	MASTEN	Mitja	Kakšno zaščito imajo naše banke
10)	NENEZIC	Vitomir	Slovenska zakonodaja na področju kriptografije in rač. varnosti
11)	NOVAK	Damjan	Twofish
12)	PIVK	Aleksander	Elektronski plačilni sistemi
13)	ROŽANEC	Alenka	Varovanje računalniških sistemov s poudarkom na zaščiti DB
14)	ŠKOF	Ivan	IDEA
15)	ŠKULJ	Janez	Kerberos
16)	TRAMPUŠ	Matej	SSL
17)	VERHOVŠEK	Roman	Javanska kriptografska knjižnica
18)	VESTER	Boštjan	Blowfish
19)	VIČIČ	Jernej	Digitalni vodni žig - digital watermark

FRI-KIRV 2002

1)	BAŠA	Vigor	Biometrija
2)	GOLOUH	Mitja	Vloga nadzora pri računalniški varnosti
3)	GROM	Matej	Varnost protokola Bluetooth
4)	JEREB	Franci	IPsec protokol v VPN omrežjih
5)	KUSTER	Robert	RNG(LFSR)/CRC
6)	MOČNIK	Jaka	E-volitve
7)	OBLAK	Boštjan	HMAC
8)	PERME	Marko	Digitalni denar
9)	POR	Luka	OpenSSL in certifikati
10)	SPINDLER	Matej	XTR kriptosistem
11)	STAJDUHAR	Ivan	DS in timestamping: Digitalni dokumenti danes
12)	STORMAN	Iztok	IPSEC/802.11b, 802.1x/UMTS
13)	UNK	Miha	Varnost mreznih naprav
14)	ZAPLOTNIK	Tomaž	Kriptografske hash funkcije
15)	ZUPAN	Janez	RNG/ključi in testi linearnosti

FMF–KITK 2003

1)	BIZJAK	Maja	Zgodovina kodiranja
2)	BREZNIK	Kristija	Elementarni dokaz praštevilskega izreka
3)	BRLOGAR	Aljoša	Dokazi brez razkritja znanja
4)	DAKSKOBLER	Blaž	Praštevilo je v P
5)	GOLJEVŠČEK	Luka	Differential power analysis
6)	IPŠA	Simona	Enigma in Purple (WWII)
7)	JERMAN	Nataša	Otroška kriptografija
8)	KIRN	Meta	Kripto-popul3
9)	KOCBEK	Primož	Kleptografija (Študij varne kraje informacij)
10)	KOMELJ	Andrej	OPEN SSL in EC
11)	KOŠIČ	Janja	Kripto-popul2
12)	KRALJ	Katarina	Fish in Tunny
13)	MAHNIČ	Jana	Konvolucijske kode
14)	MLEKUŽ	Patrik	Prehod med bazami
15)	OŽEK	Matej	WEP, 802.11i
16)	REŠČIČ	Miha	EC implementation
17)	STANEK	Maruša	Normalne baze
18)	STRAŽAR	Anja	Dokazi brez razkritja znanja
19)	ŠIRCELJ	Karin	Kripto-popul1
20)	TOLA	Špela	Kripto-krožek
21)	TOMAŠ	Tatjana	Identifikacijska števila in črtne kode
22)	URLEP	Matjaž	Varna domača stran
23)	VUKSANOVIC	Miloš	Simetrične sifre
24)	ZADRAVEC	Aleš	Vizualna kriptografija in Hadamardjeve matrike
25)	ZEMAN	Mirjana	Psevdo-naključna zaporedja
26)	ŽELJKO	Jure	Razcep polinomov
27)	ŽIBRAT	Simon	Časovne oznake

FRI–KIRV 2004

1)	ALFIREVIC	Igor	Hash funkcije
2)	BRESKVAR	Gorazd	WEP, 802.11i?
3)	DOLENC	Boštjan	Napadi na RNG
4)	DRNOVŠČEK	Slavko	Slepi podpis
5)	GLAVIC	Boris	Standard XML - XAdES
6)	JANEŽIČ	Damjan	Uporabnost moènostne identifikacije za varno e-poslovanje
7)	JERIČ	Borut	Metode preklicevanja certifikatov
8)	KLJUN	Matjaž	Hackerji
9)	KOS	Ludvik	Digitalna poštna znamka
10)	KOVAČ	Jure	Brezkontaktne sc
11)	KRALJ	Primož	Glasbena gesla
12)	MAHKOVEC	Žiga	Analiza RNG v Linuxu
13)	PAVLIČ	Tomaž	Digitalni denar
14)	PRAPROTNIK	Matjaž	CC LFSR
15)	REBOLJ	Gregor	Kriptoanaliza SIM kartice?
16)	SKUBIC	Ales	Varna soba
17)	TOMAŠEVIČ	Denis	Požarni zid v OpenBSD
18)	VIDRIH	David	E-glasovanje
19)	ZDEŠAR	Blaž	Mentalni poker

FRI–KIRV 2006

1)	HITI	Tomaž	Varnost gesel in dinamična gesla
2)	KEJŽAR	Marko	Družina zgoščevalnih funkcij SHA
3)	KERŠNIK	Jelena	Kriptosistem XTR
4)	KRMELJ	Jernej	Elektronske dražbe
5)	ŠTIMEC	Aleš	Diferenčna analiza električne aktivnosti
6)	TURK	Boris	Faktorizacija - algoritem številskega rešeta
7)	ZUPANČIČ	Tadej	Pregled varnosti pri komunikaciji z GSM

IŠRM–KITK 2008

1)	ERMENC	Rok	Dokazi brez razkritja znanja
2)	JANEŽ	Tadej	SE:crypto-engine, digitalni denar
3)	MUHIČ	Andrej	EC DLP
4)	KOŠMERLJ	Aljaz	Zgoščevalne funkcije
5)	NOSE	Peter	NTRU, EC štetje točk
6)	PAŠČINSKI	Uros	McEliece shema za podpis
7)	SIPOŠ	Ruben	TPM
8)	ŠUBELJ	Lovro	Vizualna kriptografija
9)	TRAMPUŠ	Mitja	Mentalni poker
10)	VIDALI	Janos	Skupinski podpisi
11)	ŽBONTAR	Jure	Pametne kartice
12)	ŽAGAR	Lan	Testiranje hadrwerskega RNG

FRI–KIRV 2008

1)	ANŽIN	Matej	AES - konkretna implementacija?
2)	ČERNIVEC	Aleš	Infrastruktura javnih ključev (PKI)
3)	FAJT	Radivoj	Wireless (brez WEB) in IPSec
4)	GLAD	Damjan	Lamportov podpis
5)	JUŽNA	Jernej	RC4
6)	KASTELIC	Marko	Družina zgoščevalnih funkcij SHA-2
7)	MAVER	Jan	Anonimnost podatkovnih baz
8)	MUNDA	Davor	Analiza PRNG v Linux
9)	POREKAR	Jan	Varnost dolgoročne hrambe
10)	RAZORŠEK	Grega	Nepropustnost kriptografskih naprav
11)	SOLIČ	Mirko	Digitalni denar
12)	STAJDOHAR	Miha	Dokazi brez razkritja znanja
13)	STARC	Iztok	Varnost brezkontaktih kartic
14)	TOPLAK	Marko	Zakonodaja na področju računalniške varnosti
15)	IMŠIROVIC	Denis	Požarni zid v OpenBSD

IŠRM–KITK 2009

1)	BLAGUS	Neli	Sim kartice
2)	BOGATAJ	Polona	Zgodovina kripto - Colossus
3)	KOŠMERL	Marko	Network security
4)	KOZINA	Simon	Časovni žigi
5)	MAČEK	Tina	Črtne kode
6)	MOŠKON	Sašo	Brezkontaktne kartice
7)	PEVEC	Darko	Poštna znamka
8)	POLAJNAR	Matija	Sidechannel attacks
9)	PUGELJ	Mitja	Turbo kode
10)	RADOVIC	Marija	KeeLoq
11)	STARC	Janez	Dokazi brez razkritja znanja
12)	VIDMAR	Kaja	Kid-crypto
13)	TOLIC	Andrej	HMAC

IŠRM–KITK 2010

1)	AMBROŽIČ	Martin	Pollardova ro metoda za razcep
2)	KRNC	Matjaž	Hadamardove matrike
3)	LIST	Ivo	E-volilne sheme
4)	PURGAJ	Janko	Kvantni digitalni podpis
5)	ROJKO	Mateja	Deljenje skrivnosti
6)	ŠKOFIC	Nejc	Kvantni prstni odtis
7)	STARIČ	Anže	Časovni žigi
8)	VELKAVRH	Gaja	Varnostna območja
9)	ŽITNIK	Slavko	RFID
10)	NOVAK	Matija	SET
11)	PEROVŠEK	Matic	Implementacija PRNG v FPGA
12)	UGRIN	Matej	Kriptografski protokoli

FRI–KIRV 2010

1)	BEŠTEK	Mate	TinyECC za brezžična senzorska omrežja
2)	SKALE	Primož	Varovanje splatnih strani (HTTPS)
3)	ŠKOBERNE	Nejc	Lokalizirana spletna baza zgoščenih vrednosti

IŠRM–KITK 2011

1)	ŠTEFANČIČ	Leonard	Arne Beurling in G-Schreiber v 2. svetovni vojni
2)	AZARIJA	Jernej	BitCoin
3)	SLAPNIK	Andrej	Anonimne in varne elektronske ankete s sistemom Helios
4)	MEDVEŠEK	Jure	Implementacija metode index calculus za računanje diskretnega logaritma nad praštevilskimi obsegi
5)	TRDIN	Nejc	Kriptosistem XTR z javnimi ključi
6)	ŽAGAR	Andraž	Rojstnodnevni napad

IŠRM–KITK 2012

)	ABRAMOVIČ	Maja	IPSec
)	BARTOL	Florjan	Implementacija Index Calculus metode na GPU
)	BIBLER	Tomaž	Problem kriptografov na večerji
)	BIZJAK	Ambrož	Preprečevanje DOS napadov z uporabniškimi ugankami
)	BOBEK	Gregor	Optimizacijske metode za potenciranje
)	CINDRO	Luka	Napad na Playstation3
)	COLNERIČ	Niko	Steganografski datotečni sistema StegFS
)	DAKSKOBLER	Larisa	Kriptoanaliza in načrtovanje S-škatel
)	DRAME	Matej	Kvantna faktorizacija in razbijanje DLP
)	FAJDIGA	Antonio	Certifikatna agencija na FRI
)	HARTMAN	Jernej	Implementacija napada z merjenjem časa za kriptosisteme z javnimi klj
)	KARANTAN VOZEL	Gašper	GCHQ-Ali lahko razbiješ?
)	KOBETIČ	Klemen	Analiza varnosti Enigme
)	KOLAR	Mirjam	Lehmerjev algoritem
)	KOTAR	David	Intelov strojni generator naključnih števil
)	KOVAČ	Sanja	Napadi na simetrične šifre
)	MEDVEŠEK	Urša	Napad na zgoščevalno funkcijo MD5
)	LEINER	Adrien	Anonymous remailer
)	LIBENŠEK	Sonja	Računanje diskretnega logaritma na odsekih
)	LIPNIK	Izak	Implementacija napada z analizo porabe moči na DES
)	MIKAC	Mojca	Homomorfni kriptosistemi
)	MLADOVAN	Domen	Simetrične šifre za kompresijske funkcije
)	NEDELJKO	Miha	DNSsec protokol
)	ODER	Andrej	Simetrična šifra MARS
)	PAŠČINSKI	Uroš	Shema za sledenje izdajalcem
)	PETERLIN	Blaž	Nezaveden prenos
)	PIRIH	Metka	Tokovna šifra RC4
)	POBERŽNIK	Matevž	Šifrirani piškotki in prenosljivost HTTP sej
)	ROVAN	Ana	Steganografija v TCP časovnih žigih
)	SIMONIČ	Klemen	Časovno omejeno šifiranje
)	SLOSU	Andreja	Kriptografske lastnosti Boolovih funkcij
)	STOPAR	Luka	IPSec
)	STRAŽAR	Martin	Zakonodaja na področju kriptografije in računalniške varnosti
)	ŠAULI	Jan	Zasebnost in varnost v socialnih omrežjih
)	TOMAŠIČ	Polona	Pay-per-view protokoli
)	TOPOLNJAK	Dajana	Private information retrival
)	TREBUŠAK	Matic	Evercookie | neizbrisljiv piškotek
)	VARLJEN	Jan	Honeypot za družbena omrežja
)	VIDMAR	Sandra	Napadi na simetrične šifre
)	VRHOVEC	Andraž	Analiza napake na DEBIAN OpenSSL
)	VUČKOVIČ	Miha	Commitcoin | datiranje z BitCoinom
)	WRITZL	Jerneja	Simetrična šifra TWOFISH
)	ZAPUŠEK	Gorazd	Črv Stuxnet
)	ZORKO	Robert	Primerjava in analiza SHA-3 kandidatov
)	ŽITNIK	Marinka	Zaklenjena skrivnost

IŠRM–KIRV 2017

1)	BARANEK	Martin	EC in Restricted Comput Env
2)	BENEDIK	Dejan	Linux PRNG
3)	IVANŠEK	Rok	Classifying Classical Ciphers
4)	FILIĆ	Mia	GNSS Navigation Message Authentication TESLA
5)	JANEŽIČ	Erik	Elizika
6)	KAVČIČ	Tilen	Digitalni Denar FRIKOIN
7)	KIŠEK	Nejc	Identification RFOD
8)	KLEMENČIČ	Štefan	Enigma
9)	LANGR	Filip	Mental Poker (Miselni poker)
10)	MAKOVEC	Makovec	Tokovna šifra RC4
11)	PUSNIK	Žiga	Testiranje praštevilskosti
12)	REPAŠ	Blaž	Frequency Hopping Spread Spectrum
13)	ŠTULAR	Janez	Varnost SMS
14)	ZAVRTANIK	Matej	Zgoščevalna funkcija HMAC

IŠRM–KIRV 2018

1)	BERCHER	Jason	Digital Stamp
2)	BRITVIĆ	Tihana	Attacks On ElGamal
3)	HORVAT	Matej	Serpent
4)	KERN	Žiga	Prijava_v_MS_OS_s_SC
5)	KLEMENC	David	Mining BTC
6)	MILAČIĆ	Katarina	eVoting
7)	PERRIN	Alizee	Wireless SC
8)	SCHELTEN	Niklas	SHA3
9)	SENIČIČ	Luka	Mental Poker
10)	SCHWERICKE	Anton	Crypto Currencies
11)	ŠKOBE	Mirjam	Floyd Algorithm
12)	ŠUBELJ	Jan	Anonymity Onion Routing Tor
13)	TURANJANIN	Aleksandra	SIM card

IŠRM–KIRV 2019

1)	DIESNIS	Florian	Wireless Smart Cards security (Varnost brezžičnih pametnih kartic)
2)	GAŠPERLIN	Domen	Homomorfno šifriranje
3)	LAMPIČ	Jan	Miselni poker
4)	KLANJŠČEK	Klemen	Kriptografska analiza telegramov iz 2. svetovne vojne
5)	Merljak	Jakob	Varnostni mehanizmi v sistemu Android
6)	RUS	Andrej	Floydov algoritem
7)	SOSA	Ante	Bliskovito omreže (Lightning Network)
8)	VALENTE	Joana	Algorand

IŠRM–KIRV 2020

1)	BIZJAK	Matej	Argon
2)	HARCEKOVA	Lucia	Group Blind Digital Signatures (Skupinski slepi digitalni podpisi)
3)	BURJA	Andrej	DES Fire EV1
4)	KNEZ	Timotej	Double Ratchet algoritem
5)	NUNČIČ	Aljaž	Enkratni podpisi in Marklova drevesa zgostitev
6)	METLIČAR	Samo	Generiranje močnih praštevil
7)	PEGAN	Jasmina	ElGamal in kleptografija
8)	ŠTRAVS	Miha	Miselni poker večstrankarsko računanje
9)	ABE	Gregor	Digitalni pečat
10)	BERTONCELJ	Tine	Enostavna analiza porabe energije pri RSA kriptosistemih
11)	BIZJAK	Matej	Zgoščevanje gesel s funkcijo Argon2
12)	ČOPI	Špela	Kriptografi na večerji
13)	GERŠAK	Jan	Psevdo-naključni generatorji števil na kvantnih računalnikih
14)	JAMŠEK	Miha	Nova varnostna politika za @friCA
15)	JENKO	Jan	SQL šifriranje
16)	KERŠEVAN	Gregor	NISTovo tekmovanje za izbor algoritma SHA-3 in analiza zgoščevalne funkcije BLAKE
17)	KOBAU	Klemen	Kriptosistem NTRU
18)	REBERNIK	Nejc	Zasebni ključi agencije za digitalna potrdila

IŠRM–KIRV 2021

1)	Marinko	Matej	Algoritmi za faktorizacijo celih števil
2)	BRECELJ	Bor	Anonimnost in nevidnost podpisov brez možnosti zanikanja
3)	ERZIN	Aljaž	Miselni poker
4)	TURK	Martin	Timing Attacks against TLS and DTLS
5)	FIDEL	Denis	WPA3
6)	BERTOK	...	EC
7)			Kriptografi na večerji
8)	...		
9)	...		
10)	...		
...			

IŠRM–KIRV 2022

1)	RAJH	Mihael	Subverting NIST Hash PRNG