Konkurs na najlepszą pracę magisterską i inżynierską z dziedziny kryptografii i ochrony informacji opracowaną na polskich uczelniach w latach 2003-2004

Prace nadesłane na Konkurs

- **10 prac**

- **5 miast**
- **6 uczelni**

- **1005 stron**
- **169 146 kB (po kompresji)**

Członkowie Komisji Konkursowej

Prof. Józef Pieprzyk,
Department of Mathematics
Macquarie University, Australia

dr hab. inż. Zbigniew Kotulski,
Instytut Podstawowych Problemów Techniki, PAN

dr inż. Janusz Szczepański,
Instytut Podstawowych Problemów Techniki, PAN

dr Ryszard Kossowki
Instytut Telekomunikacji Politechniki Warszawskiej

---

dr inż. Krzysztof Gaj
ECE Department, George Mason University

Członkowie Komisji Konkursowej

- 3 kontynenty
- 4 instytuty
- 5 opinii

Prace zakwalifikowane do Konkursu

10 Uczestników > 5 Członków Komisji

- **10 prac** → **4 prace** → **5 prac**

			kompresja o
• **5 miast**	→	**4 miasta**	**20 %**
• **6 uczelni**	→	**5 uczelni**	**17 %**

• **1005 stron**	→	**503 strony**	**50 %**
• **169 146 kB (.zip)**	→	**164 663 kB (.zip)**	**3 %**

Wszyscy uczestnicy konkursu
i ich Opiekunowie
uzyskali bezpłatny wstęp na konferencję
a uczestnicy zamiejscowi również
zakwaterowanie w Warszawie


1
2
3


4
2 = h (m llr)
2


Ewa Ignasiak
KUL, Lublin
Rozdział 3. Definicja po
elektronicznego w świet
września 2001 r. o podp
3.1. Pojęcie dokumen
3.2. Pojęcie podpisu
3.3. Pojęcie podpisu
3.4. Porównanie pod
z elektroniczny
Ewa Ignasiak „Definicja i f
ustawy z dnia 18 wrześ
12-05-2004

Krzysztof Gołofit
PW, Warszawa

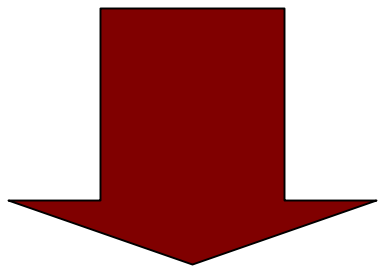
Daniel Jasionowski
Uniwersytet Sląski,
Katowice

ppor. Rafał Parzych
WAT, Warszawa


Remigiusz Towalski
PP, Poznań

W jaki sposób wyeliminować subiektywność z ocen Komisji ?

Stosować kryteria bezwzględne (liczbowe), gdzie ocena Komisji nie jest niezbędna



5 nagród specjalnych

Kategoria I
Najkrótsza praca dyplomowa…

1. Daniel Jasionowski, “Kryptoanaliza MD4” – 31 stron
2. Remigiusz Towalski, “Steganografia” – 39 stron
3. Rafał Parzych, “Analiza ataków poboru mocy…” – 99 stron
4. Ewa Ignasiak, “Definicja i funkcje podpisu…” – 121 stron
5. Krzysztof Gołofit, “Implementacja systemów podpisów” – 213 stron

Kategoria II
Najkrótsza prezentacja…

1. **Remigiusz Towalski, “Steganografia” – 5 minut**

2. **Daniel Jasionowski, “Kryptoanaliza MD4” – 7 minut**

3-5.
Ewa Ignasiak, “Definicja i funkcje podpisu…”
– 10 minut
Krzysztof Gołofit, “Implementacja systemów podpisów”
– 10 minut
Rafał Parzych, “Analiza ataków poboru mocy…”
– 10 minut

Kategoria III
Najdłuższa sesja pytań i odpowiedzi…

1. Krzysztof Gołofit, “Implementacja systemów podpisów” – 18 minut

2-4.

Ewa Ignasiak, “Definicja i funkcje podpisu…” – 10 minut

Daniel Jasionowski, “Kryptoanaliza MD4” – 10 minut

Rafał Parzych, “Analiza ataków poboru mocy…” – 10 minut

5. Remigiusz Towalski, “Steganografia” – 5 minut

Kategoria IV
Najdłuższa bibliografia…

1. Ewa Ignasiak, “Definicja i funkcje podpisu…” – 319 pozycji
2. Krzysztof Gołofit, “Implementacja systemów podpisów” – 71 pozycji
3. Remigiusz Towalski, “Steganografia” – 32 pozycje
4. Rafał Parzych, “Analiza ataków poboru mocy…” – 25 pozycji
5. Daniel Jasionowski, “Kryptoanaliza MD4” – 10 pozycji

Kategoria V
Najkrótszy tytuł…

1. **Rafał Parzych, “”**
   – 0 słów
2. **Remigiusz Towalski, “Steganografia” – 1 słowo**
3. **Daniel Jasionowski, “Kryptoanaliza MD4” – 2 słowa**
4. **Krzysztof Gołofit, “Implementacja systemów podpisów”**
   – 7 słów
5. **Ewa Ignasiak, “Definicja i funkcje podpisu…”**
   – 16 słów

WOJSKOWA AKADEMIA TECHNICZNA

im. Jarosława Dąbrowskiego

PRACA DYPLOMOWA

STUDIA WYŻSZE

ppor. Rafał Parzych

(stopień, imię i nazwisko dyplomanta)

WYDZIAŁ CYBERNETYKI

(wydział)

KRYPTOLOGIA

(specjalność)

dr inż. Piotr BORA

(stopień, imię i nazwisko kierownika pracy)

WARSZAWA - 2004


– 31 stron
– 39 stron
– 99 stron
– 121 stron
– 213 stron

Kryteria, które Komisja brała pod uwagę…

Poprawność

Optymalność

Znajomość literatury

Oryginalność

Przydatność

Prezentacja

Odpowiedzi na pytania


knows the public key pk
• the known-message attacks -
has access to a list of valid messa
pairs.
– random-message attack (RM
– chosen-message attack (CM
– a forgery of any valid signatur
in the above list. This is th
security level, a.k.a. non-mal

V nagroda

IV nagroda

III nagroda

II nagroda

I nagroda

Wszystkie nagrody
ufundowała
firma

Enigma

Systemy Ochrony Informacji

Nagrody pochodzą

z Muzeum Kryptologii Narodowej Agencji Bezpieczeństwa w Fort Mead Maryland, U.S.A


Konkurs na najlepszą pracę
magisterską i inżynierską
z dziedziny kryptografii i ochrony informacji
opracowaną
na polskich uczelniach w latach 2003-2004

V nagroda

Remigiusz Towalski

Instytut Informatyki
Wydział Informatyki i Zarządzania
Politechnika Poznańska

Opiekun pracy:

dr inż. Anna Grocholewska-Czuryło

Tytuł pracy:

“Steganografia”

IV Nagroda

Ewa Ignasiak

Wydział Prawa, Prawa Kanonicznego i Administracji
Katolicki Uniwersytet Lubelski
Kierunek: Prawo

Opiekun pracy:

dr Jacek Widło

Tytuł pracy:

"Definicja i funkcje podpisu elektronicznego
w świetle ustawy z dnia 18 września 2001r.
o podpisie elektronicznym"


IV Nagroda
Ewa Ignasiak
Opiekun pracy:
dr Jacek Widło
Tytuł pracy:

III Nagroda

Krzysztof Gołofit

Instytut Systemów Elektronicznych
Wydział Elektroniki i Technik Informacyjnych
Politechnika Warszawska

Opiekun pracy:

dr Magdalena Szeżyńska

Tytuł pracy:

“Implementacja systemów podpisów cyfrowych wykorzystujących krzywe eliptyczne”


ów Elektronicznych
niki i Technik Informacyjnych
rszawska
ezynska
systemów podpisów cyfrowych
ch krzywe eliptyczne"

II Nagroda

Rafał Parzych

Wydział Cybernetyki
Wojskowa Akademia Techniczna
im. Jarosława Dąbrowskiego w Warszawie
Specjalność: Kryptologia

Opiekun pracy:

dr inż. Piotr Bora

Tytuł pracy:

“Analiza ataków poboru mocy na wybrane algorytmy kryptograficzne”


ki
nia Techniczna
rowskiego w Warszawie
tologia
poboru mocy na wybrane
graficzne"
Smart Card
MAGAZYN
SYSTEMY IT

I Nagroda

Daniel Jasionowski

Wydział Matematyki Fizyki i Chemii
Uniwersytet Slaski

Opiekun pracy:

dr hab. Mieczysław Kula

Tytuł pracy:

“Kryptoanaliza MD4”


MAGAZYN
SYSTEMY IT

Serdecznie zapraszamy do

wzięcia

udziału w kolejnej edycji

konkursu

już za rok