

Spis tematów prac dyplomowych magisterskich na rok akademicki 2019/2020

	Temat	L. wyk.	Opiekun (konsultant)
1.	Rezerwacja zasobów optycznych w sieciach wielodomenowych w architekturze sieci ASON/GMPLS	1	S. Kaczmarek (M. Młynarczuk)
2.	Model symulacyjny dla architektury ASON/GMPLS z mechanizmem zabezpieczenia ścieżki optycznej	1	S. Kaczmarek (M. Młynarczuk)
3.	Analityczny model obsługi ruchu w wielodomenowej sieci IMS/NGN obejmujący warstwę usług i warstwę transportową	1	S. Kaczmarek (M. Sac)
4.	Projektowanie elementów wielodomenowej architektury IMS/NGN	1	S. Kaczmarek (M. Sac)
5.	Przegląd i badanie algorytmów szyfrowania homomorficznego	1	R. Rykaczewski
6.	Przegląd i badanie metod watermarkingu obrazów nieruchomych wykorzystujących dekompozycję SVD	1	R. Rykaczewski
7.	Przegląd i badanie modyfikacji szyfru Hilla	1	R. Rykaczewski
8.	Przegląd i badanie właściwości algorytmów odwracalnego ukrywania danych w zaszyfrowanych obrazach	1	R. Rykaczewski
9.	Aplikacja demonstrująca transmisję danych z kluczowaniem szybszym od szybkości Nyquista	1	M. Blok
10.	Badanie algorytmu Single Bit Flipping w zastosowaniu do dekodowania kodów LDPC	1	M. Blok
11.	Przegląd metod wyznaczania odpowiedzi impulsowych kanałów telekomunikacyjnych	1	M. Blok
12.	Laboratorium infrastruktury klucza publicznego	1	B. Czaplewski
13.	Laboratorium metod cyfrowego odcisku palca	1	B. Czaplewski
14.	Laboratorium jednokierunkowych funkcji skrótu	1	B. Czaplewski
15.	Przegląd i badanie właściwości wybranych modyfikacji dla algorytmu AES	1	M. Dzwonkowski
16.	Implementacja programowa i badanie kwaternionowego szyfru Hilla	1	M. Dzwonkowski
17.	Architektura routingu segmentowego	1	M. Narloch
18.	Analiza rozwiązań Message Oriented Middleware dla serwerów telekomunikacyjnych	1	M. Narloch
19.	Analiza możliwości transmisyjnych pasywnych sieci optycznych następnej generacji	1	L. Smoleński
20.	Techniki transmisji z bardzo dużą szybkością w sieci dostępowej z miedzianymi parami symetrycznymi	1	L. Smoleński
21.	Metody pomiaru jakości dla koherentnej transmisji optycznej z bardzo dużą szybkością	1	L. Smoleński

UWAGA: Pełny opis każdego tematu znajduje się także na stronie WWW Katedry
<http://eti.pg.edu.pl/katedra-sieci-teleinformatycznych/prace-dyplomowe>

[Zasady wyboru i przydziału tematu](#) są zamieszczone na końcu tego opisu.

Temat pracy dyplomowej magisterskiej (jęz. pol.)	Rezerwacja zasobów optycznych w sieciach wielodomenowych w architekturze sieci ASON/GMPLS
Temat pracy dyplomowej magisterskiej (jęz. ang.)	Optical resource reservation in multidomain ASON/GMPLS network architecture
Opiekun pracy	dr hab. inż. Sylwester Kaczmarek
Konsultant pracy	mgr inż. Magdalena Młynarczuk
Cel pracy	Zaproponowanie mechanizmów rezerwacji dla optycznych sieci wielodomenowych architektury ASON/GMPLS.
Zadania do wykonania	<ol style="list-style-type: none"> 1. Studia literaturowe w zakresie koncepcji płaszczyzny sterowania ASON/GMPLS. 2. Zapoznanie się z symulatorem architektury ASON/GMPLS. 3. Propozycja mechanizmów rezerwacji zasobów optycznych dla sieci wielodomenowych. 4. Implementacja mechanizmów rezerwacji. 5. Przeprowadzenie symulacji dla zaproponowanych mechanizmów. 6. Opracowanie wyników symulacji i sformułowanie wniosków.
Źródła	<ol style="list-style-type: none"> 1. Dokumenty standaryzacyjne architektury ASON/GMPLS 2. Kaczmarek S., Młynarczuk M., Szałajda K., <i>Performance of ASON/GMPLS architecture in condition of wavelength conversion and without wavelength conversion</i>, Przegląd Telekomunikacyjny + Wiadomości Telekomunikacyjne, nr 7, 2016. s. 653-657 3. OMNeT++ Network Simulation Framework, www.omnetpp.org 4. Prace dyplomowe magisterskie realizowane w Katedrze Sieci Teleinformatycznych.
Liczba wykonawców	1
Uwagi	Praca analityczno-programistyczna

Temat pracy dyplomowej magisterskiej (jęz. pol.)	Model symulacyjny dla architektury ASON/GMPLS z mechanizmem zabezpieczenia ścieżki optycznej
Temat pracy dyplomowej magisterskiej (jęz. ang.)	ASON/GMPLS architecture simulation model with optical connection protection mechanism
Opiekun pracy	dr hab. inż. Sylwester Kaczmarek
Konsultant pracy	mgr inż. Magdalena Młynarczuk
Cel pracy	Zaproponowanie modelu symulacyjnego dla architektury ASON/GMPLS z mechanizmem zabezpieczenia ścieżki optycznej
Zadania do wykonania	<ol style="list-style-type: none"> 1. Studia literaturowe w zakresie koncepcji płaszczyzny sterowania ASON/GMPLS. 2. Zapoznanie się z symulatorem architektury ASON/GMPLS. 3. Propozycja mechanizmu zabezpieczenia ścieżki optycznej. 4. Implementacja mechanizmu zabezpieczenia ścieżki optycznej. 5. Przeprowadzenie symulacji dla zaproponowanego mechanizmu zabezpieczenia. 6. Opracowanie wyników symulacji i sformułowanie wniosków.
Źródła	1. Dokumenty standaryzacyjne architektury ASON/GMPLS

	<p>2. Kaczmarek S., Młynarczuk M., Szałajda K., <i>Performance of ASON/GMPLS architecture in condition of wavelength conversion and without wavelength conversion</i>, Przegląd Telekomunikacyjny + Wiadomości Telekomunikacyjne, nr 7, 2016. s. 653-657</p> <p>3. OMNeT++ Network Simulation Framework, www.omnetpp.org</p> <p>4. Prace dyplomowe magisterskie realizowane w Katedrze Sieci Teleinformatycznych.</p>
Liczba wykonawców	1
Uwagi	Praca analityczno-programistyczna

Temat pracy dyplomowej magisterskiej (jęz. pol.)	Analityczny model obsługi ruchu w wielodomenowej sieci IMS/NGN obejmujący warstwę usług i warstwę transportową
Temat pracy dyplomowej magisterskiej (jęz. ang.)	Analytical traffic model of a multidomain IMS/NGN including service and transport stratum
Opiekun pracy	dr hab. inż. Sylwester Kaczmarek
Konsultant pracy	mgr inż. Maciej Sac
Cel pracy	Integracja opracowanych analitycznych modeli obsługi ruchu dla warstwy usług i warstwy transportowej IMS/NGN dla wybranej technologii warstwy transportowej (Ethernet, MPLS, FSA).
Zadania do wykonania	<p>1. Analiza literatury dotyczącej systemu IMS/NGN, w tym miar wydajności przetwarzania żądań usług oraz technologii mających zastosowanie do realizacji warstwy transportowej.</p> <p>2. Przegląd istniejących analitycznych modeli obsługi ruchu przez warstwę usług i transportową sieci IMS/NGN, w tym zapoznanie się z modelami opracowanymi w Katedrze Sieci Teleinformatycznych.</p> <p>3. Opracowanie koncepcji integracji oraz integracja modelu warstwy usług z modelem warstwy transportowej dla wybranej technologii.</p> <p>4. Przeprowadzenie badań z wykorzystaniem zintegrowanego modelu i analiza ich wyników.</p> <p>5. Przedstawienie wniosków i dalszych niezbędnych prac.</p>
Źródła	<p>1. Dokumenty standaryzacyjne architektury IMS/NGN (ITU-T, ETSI, 3GPP, IETF, IEEE i inne)</p> <p>2. Prace dyplomowe magisterskie i inżynierskie realizowane w Katedrze Sieci Teleinformatycznych</p> <p>3. S. Kaczmarek, M. Sac, Traffic model of a multidomain IMS/NGN, PTiWT, nr 8-9, 2014, pp.1030-1038</p>
Liczba wykonawców	1
Uwagi	Praca analityczno-programistyczna.

Temat pracy dyplomowej magisterskiej (jęz. pol.)	Projektowanie elementów wielodomenowej architektury IMS/NGN
Temat pracy dyplomowej magisterskiej (jęz. ang.)	Design of a multidomain IMS/NGN architecture elements
Opiekun pracy	dr hab. inż. Sylwester Kaczmarek
Konsultant pracy	mgr inż. Maciej Sac

Cel pracy	Zaproponowanie, implementacja i przebadanie sposobu projektowania elementów warstwy usług wielodomenowej sieci IMS/NGN pod kątem zapewnienia zadanych parametrów jakościowych.
Zadania do wykonania	1. Przegląd literatury dotyczącej sieci IMS/NGN. 2. Analiza parametrów charakteryzujących jakość w sieci IMS/NGN. 3. Przegląd modeli obsługi ruchu w sieci IMS/NGN. 4. Zaproponowanie sposobu projektowania elementów warstwy usług wielodomenowej IMS/NGN. 5. Implementacja oprogramowania i przeprowadzenie badań.
Źródła	1. Dokumenty standaryzacyjne architektury IMS/NGN (ITU-T, ETSI, 3GPP, IETF, IEEE i inne) 2. Prace dyplomowe magisterskie i inżynierskie realizowane w Katedrze Sieci Teleinformatycznych 3. Zasoby Internetu.
Liczba wykonawców	1
Uwagi	Praca analityczno-programistyczna.

Temat pracy dyplomowej magisterskiej (jęz. pol.)	Przegląd i badanie algorytmów szyfrowania homomorficznego
Temat pracy dyplomowej magisterskiej (jęz. ang.)	Review and research of homomorphic ciphers algorithms
Opiekun pracy	dr hab. inż. Roman Rykaczewski
Konsultant pracy	j.w.
Cel pracy	Zapoznanie się z szyfrowaniem homomorficznym, oprogramowanie wybranego algorytmu i badanie jego właściwości
Zadania do wykonania	1. Wykonanie przeglądu literatury 2. Wykonanie oprogramowania realizującego wybrany algorytm 3. Przygotowanie ćwiczenia laboratoryjnego
Źródła	1. Abbas Acar i inn.: A Survey on Homomorphic Encryption Schemes: Theory and Implementation; ACM Computing Surveys, Vol. 51, No. 4, July 2018. 2. Zasoby Internetu
Liczba wykonawców	1
Uwagi	Podana pozycja literatury powinna stanowić punkt wyjścia do przeprowadzenia poszukiwań literatury w Internecie. Oprogramowanie powinno być wykonane w środowisku Matlab

Temat pracy dyplomowej magisterskiej (jęz. pol.)	Przegląd i badanie metod watermarkingu obrazów nieruchomych wykorzystujących dekompozycję SVD
Temat pracy dyplomowej magisterskiej (jęz. ang.)	Review and research still images watermarking methods using SVD
Opiekun pracy	dr hab. inż. Roman Rykaczewski
Konsultant pracy	j.w.
Cel pracy	Wykonanie przeglądu najnowszych algorytmów, oprogramowanie wybranej metody
Zadania do wykonania	1. Wykonanie przeglądu algorytmów 2. Wykonanie oprogramowania realizującego wybrany algorytm 3. Przeprowadzenie badań za pomocą wykonanego programu
Źródła	1. Heng Zhang, Chengyou Wang, Xiao Zhou: A Robust Image Watermarking Scheme Based on SVD in the Spatial Domain, Future Internet 2017,9,45 2. Zasoby Internetu
Liczba wykonawców	1

Uwagi	Podana pozycja literatury powinna stanowić punkt wyjścia do przeprowadzenia poszukiwań literatury w Internecie. Oprogramowanie powinno być wykonane w środowisku Matlab
--------------	---

Temat pracy dyplomowej magisterskiej (jęz. pol.)	Przegląd i badanie modyfikacji szyfru Hilla
Temat pracy dyplomowej magisterskiej (jęz. ang.)	Review and research Hill cipher modifications
Opiekun pracy	dr hab. inż. Roman Rykaczewski
Konsultant pracy	j.w.
Cel pracy	Wykonanie przeglądu modyfikacji zwiększających bezpieczeństwo szyfru Hilla, oprogramowanie wybranych metod
Zadania do wykonania	1. Wykonanie przeglądu algorytmów 2. Wykonanie oprogramowania realizującego wybrane algorytmy 3. Przeprowadzenie badań za pomocą wykonanych programów.
Źródła	1. M. Nordin i inn.: Cryptography: A New Approach of Classical Hill Cipher, International Journal of Security and Its Applications, Vol. 7, No. 2, March, 2013 2. Zasoby Internetu
Liczba wykonawców	1
Uwagi	Podana pozycja literatury powinna stanowić punkt wyjścia do przeprowadzenia poszukiwań literatury w Internecie. Oprogramowanie powinno być wykonane w środowisku Matlab

Temat pracy dyplomowej magisterskiej (jęz. pol.)	Przegląd i badanie właściwości algorytmów odwracalnego ukrywania danych w zaszyfrowanych obrazach
Temat pracy dyplomowej magisterskiej (jęz. ang.)	Review and research of algorithms of reversible data hiding in encrypted images
Opiekun pracy	Dr hab. inż. Roman Rykaczewski
Konsultant pracy	j.w.
Cel pracy	Zapoznanie się z metodami odwracalnego ukrywania danych w zaszyfrowanych obrazach i ich właściwościami
Zadania do wykonania	1. Wykonanie przeglądu algorytmów 2. Wykonanie oprogramowania realizującego wybrany algorytm 3. Przeprowadzenie badań za pomocą wykonanego oprogramowania.
Źródła	1. Kaimeng Chen, Chin-Chen Chang: Real-Time Error-Free Reversible Data Hiding in Encrypted Images Using (7, 4) Hamming Code and Most Significant Bit Prediction, Symmetry 2019, 11, 51; doi:10.3390/sym11010051 www.mdpi.com/journal/symmetry 2. Zasoby Internetu
Liczba wykonawców	1
Uwagi	Podana pozycja literatury powinna stanowić punkt wyjścia do przeprowadzenia poszukiwań literatury w Internecie. Oprogramowanie powinno być wykonane w środowisku Matlab

Temat pracy dyplomowej magisterskiej (jęz. pol.)	Aplikacja demonstrująca transmisję danych z kluczowaniem szybszym od szybkości Nyquista
Temat pracy dyplomowej magisterskiej (jęz. ang.)	An application demonstrating a data transmission with Faster-Than-Nyquist signaling
Opiekun pracy	dr hab. inż. Marek Blok, prof. nadzw. PG

Konsultant pracy	
Cel pracy	Zapoznanie się z techniką FTN (<i>Faster-Than-Nyquist signaling</i> - kluczkowanie szybsze od szybkości Nyquista) i przygotowanie oprogramowania pozwalającego na badanie właściwości systemu transmisji danych wykorzystującego tę technikę i porównanie go z systemem pracującym zgodnie z kryterium Nyquista.
Zadania do wykonania	<ol style="list-style-type: none"> 1. Przegląd literatury dotyczącej realizacji transmisji danych techniką FTN, 2. Projekt, implementacja i testowanie komputerowej implementacji referencyjnego systemu transmisji danych zgodnego z kryterium Nyquista pracującego w paśmie akustycznym, 3. Projekt, implementacja i testowanie komputerowej implementacji systemu transmisji danych wykorzystującego technikę FTN pracującego w paśmie akustycznym, 4. Opracowanie aplikacji umożliwiająca badanie właściwości oraz porównywanie systemów transmisji zgodnego z kryterium Nyquista oraz bazującego na technice FTN, 5. Przygotowanie scenariuszy laboratoryjnych wykorzystujących opracowane oprogramowanie.
Źródła	<ol style="list-style-type: none"> 1. Fan, J., Guo, S., Zhou, X., Ren, Y., Li, G. Y., & Chen, X. (2017). Faster-than-Nyquist signaling: An overview. <i>IEEE Access</i>, 5, 1925-1940. 2. Landau, L., Dorpinghaus, M., & Fettweis, G. (2015, October). Communications employing 1-bit quantization and oversampling at the receiver: Faster-than-Nyquist signaling and sequence design. In <i>Ubiquitous Wireless Broadband (ICUWB), 2015 IEEE International Conference on</i> (pp. 1-5). IEEE. 3. Ishihara, T., & Sugiura, S. (2017). Faster-than-Nyquist signaling with index modulation. <i>IEEE Wireless Communications Letters</i>, 6(5), 630-633. 4. Anderson, J. B., Rusek, F., & Öwall, V. (2013). Faster-than-Nyquist signaling. <i>Proceedings of the IEEE</i>, 101(8), 1817-1830. 5. D. Dasalukunte, V. Öwall, F. Rusek, J.B. Anderson, "Faster than Nyquist Signaling", Springer, 2014
Liczba wykonawców	1
Uwagi	

Temat pracy dyplomowej magisterskiej (jęz. pol.)	Badanie algorytmu Single Bit Flipping w zastosowaniu do dekodowania kodów LDPC
Temat pracy dyplomowej magisterskiej (jęz. ang.)	Investigation of Single Bit Flipping algorithm in application to LDPC codes decoding
Opiekun pracy	dr hab. inż. Marek Blok, prof. nadzw. PG
Konsultant pracy	
Cel pracy	Zapoznanie się z kodami LDPC (<i>low density parity check</i>) i algorytmami ich dekodowania ze szczególnym uwzględnieniem algorytmu Single Bit Flipping (SBF).
Zadania do wykonania	<ol style="list-style-type: none"> 1. Zapoznanie się z koncepcją kodów LDPC; 2. Zebranie informacji na temat metod generacji macierzy testów kodów LDPC. Opracowanie narzędzia generującego

	<p>takie macierzy i pozwalającego na badanie ich właściwości;</p> <p>3. Implementacja algorytmu SBF, jego badanie oraz testowanie jego modyfikacji;</p> <p>4. Implementacja i testowanie wybranych rozwiązań miękko-decyzyjnego dekodowania kodów LDPC i porównanie ich wydajności z algorytmem SBF;</p>
Źródła	<p>1. W. E. Ryan, An introduction to LDPC codes, in CRC Handbook for Coding and Signal Processing for Recording Systems, CRC, 2005;</p> <p>2. Shokrollahi, A. (2003). LDPC codes: An introduction. Digital Fountain, Inc., Tech. Rep, 2.</p> <p>3. Addi S., Berkami A., Azouaoui A, Belkasmi M.: New Hard Decision Decoder of LDPC Codes Using Single Bit Flipping Algorithm, IEEE In Wireless Networks and Mobile Communications (WINCOM), International Conference on pp. 1-5, November 2017.</p> <p>4. W. Sułek, Kody LDPC efektywnie dekodowane w strukturach programowanych, rozprawa doktorska, Politechnika Śląska;</p> <p>5. D. Myszk (2018), Kodowanie i dekodowanie kodów LDPC, praca dyplomowa inżynierska, WETI, PG.</p>
Liczba wykonawców	1
Uwagi	

Temat pracy dyplomowej magisterskiej (jęz. pol.)	Przegląd metod wyznaczania odpowiedzi impulsowych kanałów telekomunikacyjnych
Temat pracy dyplomowej magisterskiej (jęz. ang.)	Review of methods for measurements of impulse responses of telecommunication channels
Opiekun pracy	dr hab. inż. Marek Blok, prof. nadzw. PG
Konsultant pracy	
Cel pracy	Zapoznanie się z metodami wyznaczania odpowiedzi impulsowych kanałów telekomunikacyjnych. Implementacja i badanie wybranych rozwiązań spotykanych w literaturze.
Zadania do wykonania	<p>1. Zapoznanie się z algorytmami służącymi do wyznaczania odpowiedzi impulsowych kanałów telekomunikacyjnych prezentowanych w literaturze;</p> <p>2. Opracowanie opisu wybranych metod wyznaczania odpowiedzi impulsowych kanałów telekomunikacyjnych;</p> <p>3. Przygotowanie testowych implementacji wybranych metod wyznaczania odpowiedzi impulsowych kanałów telekomunikacyjnych;</p> <p>4. Badanie właściwości wybranych metod wyznaczania odpowiedzi impulsowych kanałów telekomunikacyjnych;</p>
Źródła	<p>1. Holters, M., Corbach, T., & Zölzer, U. (2009, September). Impulse response measurement techniques and their applicability in the real world. In Proceedings of the 12th International Conference on Digital Audio Effects (DAFx-09).</p> <p>2. Rabaste, O., & Chonavel, T. (2007). Estimation of multipath channels with long impulse response at low SNR via an MCMC method. IEEE Transactions on Signal Processing, 55(4), 1312-</p>

	<p>1325.</p> <p>3. Tkac, A., & Wieser, V. (2014, May). Channel estimation using measurement of channel impulse response. In 2014 ELEKTRO (pp. 113-117). IEEE.</p> <p>4. Barbarossa, S., & Swami, A. (2001). Estimation of time-varying multipath channel parameters using chirp signals. In Proceedings. 2001 IEEE International Symposium on Information Theory (IEEE Cat. No. 01CH37252) (p. 91). IEEE.</p> <p>5. Meng, Q., Sen, D., Wang, S., & Hayes, L. (2008, December). Impulse response measurement with sine sweeps and amplitude modulation schemes. In 2008 2nd International Conference on Signal Processing and Communication Systems (pp. 1-5). IEEE.</p> <p>6. Blok, M., Zaawansowane przetwarzanie sygnałów cyfrowych; wykład i laboratorium, EiT, studia magisterskie sem 2 i 3.</p>
Liczba wykonawców	1
Uwagi	

Temat pracy dyplomowej magisterskiej (jęz. pol.)	Laboratorium infrastruktury klucza publicznego
Temat pracy dyplomowej magisterskiej (jęz. ang.)	Laboratory of public key infrastructure
Opiekun pracy	dr inż. Bartosz Czaplewski
Konsultant pracy	
Cel pracy	Celem pracy jest realizacja laboratorium badawczego zajmującego się tematyką infrastruktury klucza publicznego. Laboratorium powinno umożliwiać szyfrowanie i deszyfrowanie za pomocą wybranych algorytmów kryptografii asymetrycznej, demonstrację działania centrum certyfikacji i łańcucha certyfikacji, składanie oraz weryfikację podpisu cyfrowego, oraz przeprowadzenia ataku na słabe punkty systemu.
Zadania do wykonania	<ol style="list-style-type: none"> 1. Poznanie zagadnień kryptografii asymetrycznej. 2. Dokonanie wyboru środowiska oraz języka programowania. 3. Implementacja poszczególnych elementów systemu, m.in. aplikacji użytkowników, centrum certyfikacji, itp. 4. Przygotowanie scenariuszy dydaktycznych na podstawie przygotowanego stanowiska laboratoryjnego.
Źródła	<ol style="list-style-type: none"> 1. Specyfikacja wybranych algorytmów kryptografii asymetrycznej 2. Bartosz Czaplewski, „Bezpieczeństwo Systemów Informatycznych” – wykład 3. Internet 4. Dokumentacja techniczna wybranego języka programowania
Liczba wykonawców	
Uwagi	

Temat pracy dyplomowej magisterskiej (jęz. pol.)	Laboratorium metod cyfrowego odcisku palca
---	--

Temat pracy dyplomowej magisterskiej (jęz. ang.)	Laboratory of digital fingerprint methods
Opiekun pracy	dr inż. Bartosz Czaplewski
Konsultant pracy	
Cel pracy	Celem pracy jest realizacja laboratorium badawczego zajmującego się tematyką metod cyfrowego odcisku palca. Laboratorium powinno umożliwiać osadzanie odcisków palca w danych za pomocą wybranych algorytmów, realizację ataków na odciski palca, wydobywanie odcisków palca z danych oraz identyfikację użytkowników zamieszczanych w atak.
Zadania do wykonania	<ol style="list-style-type: none"> 1. Poznanie zagadnień metod cyfrowego odcisku palca. 2. Dokonanie wyboru środowiska oraz języka programowania. 3. Implementacja poszczególnych elementów systemu, m.in. strony dystrybucyjnej, strony klienta, strony realizującej detekcję i identyfikację, itp. 4. Przygotowanie scenariuszy dydaktycznych na podstawie przygotowanego stanowiska laboratoryjnego.
Źródła	<ol style="list-style-type: none"> 1. Specyfikacja wybranych algorytmów metod cyfrowego odcisku palca. 2. Bartosz Czaplewski, „Bezpieczeństwo Systemów Informatycznych” – wykład 3. Internet 4. Dokumentacja techniczna wybranego języka programowania 5. Bartosz Czaplewski, „Nowe metody łącznego fingerprintingu i deszyfracji do zabezpieczania obrazów kolorowych”, rozprawa doktorska
Liczba wykonawców	
Uwagi	

Temat pracy dyplomowej magisterskiej (jęz. pol.)	Laboratorium jednokierunkowych funkcji skrótu
Temat pracy dyplomowej magisterskiej (jęz. ang.)	Laboratory of one-way hash functions
Opiekun pracy	dr inż. Bartosz Czaplewski
Konsultant pracy	
Cel pracy	Celem pracy jest realizacja laboratorium badawczego zajmującego się tematyką jednokierunkowych funkcji skrótu. Laboratorium powinno umożliwiać demonstrację różnych zastosowań funkcji skrótu, m.in. uwierzytelnianie wiadomości, podpis cyfrowy, bezpieczne przechowywanie haseł użytkowników, itp. Laboratorium powinno także umożliwiać realizację ataków na funkcje skrótu, m.in. atak poprzez kolizję, atak za pomocą tęczyowych tablic, oraz atak brutalny.
Zadania do wykonania	<ol style="list-style-type: none"> 1. Poznanie zagadnień jednokierunkowych funkcji skrótu. 2. Dokonanie wyboru środowiska oraz języka programowania. 3. Implementacja poszczególnych elementów systemu. 4. Przygotowanie scenariuszy dydaktycznych na podstawie przygotowanego stanowiska laboratoryjnego.
Źródła	1. Specyfikacja wybranych algorytmów kryptografii asymetrycznej

	2. Bartosz Czapplewski, „Bezpieczeństwo Systemów Informatycznych” – wykład 3. Internet 4. Dokumentacja techniczna wybranego języka programowania
Liczba wykonawców	
Uwagi	

Temat pracy dyplomowej magisterskiej (jęz. pol.)	Przegląd i badanie właściwości wybranych modyfikacji dla algorytmu AES
Temat pracy dyplomowej magisterskiej (jęz. ang.)	Review and examination of properties of selected modifications for the AES algorithm
Opiekun pracy	dr inż. Mariusz Dzwonkowski
Konsultant pracy	
Cel pracy	Dokonanie przeglądu metod zwiększających bezpieczeństwo i wydajność algorytmu AES, zaimplementowanie i przebadanie wybranych modyfikacji.
Zadania do wykonania	<ol style="list-style-type: none"> 1. Przegląd literatury modyfikacji algorytmu AES. 2. Opis procesu szyfrowania i deszyfrowania algorytmu AES z wybranymi modyfikacjami. 3. Implementacja, w środowisku Matlab, algorytmu AES i wybranych modyfikacji. 4. Przeprowadzenie badań i testów. 5. Ułożenie ćwiczenia laboratoryjnego prezentującego właściwości zastosowanych modyfikacji.
Źródła	<ol style="list-style-type: none"> 1. Daemen J., Rijmen V., <i>AES Proposal: Rijndael</i> 2. Niharika Tyagi, Priyanka, <i>A Survey on Ensemble of Modifications on AES Algorithm</i>, Journal of Basic and Applied Engineering Research, 1 (7), 2014, s. 19-24. 3. Czapplewski B., <i>Bezpieczeństwo Systemów Informatycznych</i> – wykład 4. Internet
Liczba wykonawców	1
Uwagi	

Temat pracy dyplomowej magisterskiej (jęz. pol.)	Implementacja programowa i badanie kwaternionowego szyfru Hilla
Temat pracy dyplomowej magisterskiej (jęz. ang.)	Software implementation and research of the quaternion Hill cipher
Opiekun pracy	dr inż. Mariusz Dzwonkowski
Konsultant pracy	
Cel pracy	Zbadanie właściwości kwaternionów dla zastosowań kryptograficznych. Zaimplementowanie i przebadanie kwaternionowej wersji szyfru Hilla.
Zadania do wykonania	<ol style="list-style-type: none"> 1. Zapoznanie się z literaturą algebry kwaternionowej. 2. Opis procesu szyfrowania i deszyfrowania dla tradycyjnego i kwaternionowego szyfru Hilla. 3. Implementacja, w środowisku Matlab, kwaternionowego szyfru Hilla.

	4. Przeprowadzenie badań i testów.
Źródła	<ol style="list-style-type: none"> 1. T. Nagase, M. Komata, T. Araki, 'Secure Signals Transmission Based on Quaternion Encryption Scheme', IEEE Advanced Inf. Netw. and Applications (AINA 2004), vol. 2, pp. 35-38. 2. F. Zhang, 'Quaternion and Matrices of Quaternions', Linear Algebra and its Applications, Elsevier Science Inc. 1997, pp. 21-57. 3. R. Goldman, 'Understanding Quaternions', Graphical Models, 2011, 73, (2), pp. 21-49. 4. D. Eberly, 'Quaternion Algebra and Calculus', Geometric Tools, LLC, 2010. 5. B. Czaplewski, <i>Bezpieczeństwo Systemów Informatycznych</i> – wykład 6. Internet
Liczba wykonawców	1
Uwagi	

Temat pracy dyplomowej magisterskiej (jęz. pol.)	Architektura routingu segmentowego
Temat pracy dyplomowej magisterskiej (jęz. ang.)	Segment Routing architecture
Opiekun pracy	dr inż. Marcin Narloch
Konsultant pracy	
Cel pracy	Celem pracy jest analiza procesu standaryzacji oraz stanu wiedzy i implementacji systemu routingu segmentowego - nowatorskiej propozycji realizacji sterowania strumieniami informacji w sieciach IP łączącego najlepsze cechy routingu IP, architektury MPLS oraz koncepcji SDN (Software Defined Network).
Zadania do wykonania	<ol style="list-style-type: none"> 1. Zapoznanie się z dotychczasowymi sposobami sterowania strumieniami pakietów w sieciach IP w kontekście architektury routingu segmentowego; 2. Zapoznanie się i analiza procesu standaryzacji architektury routingu segmentowego 3. Przegląd literaturowy wybranych publikacji poświęconych architektury routingu segmentowego 4. Analiza rozwiązań (w szczególności open source) dla praktycznej realizacji architektury routingu segmentowego; 5. Opracowanie koncepcji implementacji architektury routingu segmentowego z wykorzystaniem metod symulacyjnych oraz emulatorów sieci IP
Źródła	<ol style="list-style-type: none"> 1. Filsfils C. et al.: <i>Segment Routing Architecture, draft-ietf-spring-segment-routing-14</i>, IETF RFC 8402, July, 2018. 2. dokumenty standaryzacyjne grupy roboczej IETF SPRING (Source Packet Routing in Networking) 3. Cianfrani A.; Listanti M; Polverini M.: <i>Incremental Deployment of Segment Routing Into an ISP Network: a Traffic Engineering Perspective</i>, IEEE/ACM Transactions on Networking, August 2017.

Liczba wykonawców	
Uwagi	

Temat pracy dyplomowej magisterskiej (jęz. pol.)	Analiza rozwiązań Message Oriented Middleware dla serwerów telekomunikacyjnych
Temat pracy dyplomowej magisterskiej (jęz. ang.)	Analysis of Message Oriented Middleware for telecommunication servers
Opiekun pracy	dr inż. Marcin Narloch
Konsultant pracy	
Cel pracy	Celem pracy jest analiza rozwiązań Message Oriented Middleware (MOM) w zakresie dostępnych funkcjonalności, wspieranych protokołów oraz określenie środowiska dla przeprowadzenia testów wydajności.
Zadania do wykonania	<ol style="list-style-type: none"> 1. Zapoznanie się z koncepcją komunikacji z wykorzystaniem przesyłania wiadomości. 2. Przegląd koncepcji, protokołów i rozwiązań MOM 3. Przegląd i ocena wybranych implementacji MOM w zakresie bibliotek komunikacyjnych oprogramowania klienckiego i serwerów (brokerów) wiadomości. 4. Zaproponowanie koncepcji testów i środowiska dla przeprowadzenia testów wydajności wybranych implementacji MOM. 5. Wykonanie testów i ocena uzyskanych wyników.
Źródła	<ol style="list-style-type: none"> 1. Mahmoud Q. (ed.), Middleware for Communications, Wiley, 2005. 2. Chappell D., Enterprise Service Bus, O'Reilly, 2004 3. Strony WWW i dokumentacja rozwiązań MOM. 4. Sach. K., Kounev S., Bacon J. Buchmann A., Performance evaluation of message-oriented middleware using the SPECjms2007 benchmark, Performance Evaluation Vol. 66, Issue 8, August 2009, pp. 410-434. 5. ETSI TS 186 008-1 IMS Network Testing (INT)); IMS/NGN Performance Benchmark, 2012.
Liczba wykonawców	
Uwagi	

Temat pracy dyplomowej magisterskiej (jęz. pol.)	Analiza możliwości transmisyjnych pasywnych sieci optycznych następnej generacji
Temat pracy dyplomowej magisterskiej (jęz. ang.)	Analysis of next-generation passive optical network transmission capabilities
Opiekun pracy	Lech Smoleński
Konsultant pracy	-
Cel pracy	Ocena możliwości transmisyjnych pasywnych sieci optycznych następnej generacji, analiza porównawcza parametrów i możliwości wykorzystania w optycznej sieci dostępowej.
Zadania do wykonania	1. Przegląd technik stosowanych w szerokopasmowych pasywnych sieciach optycznych następnej generacji.

	2. Identyfikacja i ocena liczbowa czynników ograniczających szybkość i zasięg transmisji dla analizowanych szerokopasmowych sieci PON. 3. Porównanie uzyskiwanych parametrów i możliwości wykorzystania analizowanych rozwiązań PON w optycznej sieci dostępowej.
Źródła	1. insight.nokia.com/xgs-pon-makes-ng-pon-simpler (05/2019) 2. insight.nokia.com/twdm-pon-taking-fiber-new-wavelengths (05/2019) 3. ITU-T, Rec. G.98xx
Liczba wykonawców	1
Uwagi	

Temat pracy dyplomowej magisterskiej (jęz. pol.)	Techniki transmisji z bardzo dużą szybkością w sieci dostępowej z miedzianymi parami symetrycznymi
Temat pracy dyplomowej magisterskiej (jęz. ang.)	Transmission techniques with very high speed in the access network with copper symmetrical pairs
Opiekun pracy	Lech Smoleński
Konsultant pracy	-
Cel pracy	Analiza technik wykorzystywanych dla transmisji z bardzo dużymi przepływnościami w sieci dostępowej korzystającej z miedzianych par symetrycznych, ocena ograniczeń transmisji i możliwości wykorzystania w sieci dostępowej.
Zadania do wykonania	1. Przegląd technik stosowanych w transmisji z bardzo dużymi szybkościami w sieci dostępowej z miedzianymi parami symetrycznymi. 2. Identyfikacja i ocena wpływu czynników ograniczających szybkość i zasięg transmisji dla analizowanych rozwiązań. 3. Ocena możliwości wykorzystania analizowanych rozwiązań w sieci dostępowej.
Źródła	1. ITU-T: Rec. G.9701, Fast access to subscriber terminals (G.fast) – Physical layer specification, 12/2014; 2. Conneally P, Johnson J. New ITU broadband standard fast-tracks route to 1Gbit/s. ITU-T Press Release, Geneva 2013; 3. Coomans W. i in.: XG-FAST: Towards 10 Gb/s copper access, 2014 IEEE Globecom Workshops. 4. Coomans W. i in.: XG-fast: the 5th generation broadband, IEEE Communications Magazine, vol. 53, Dec. 2015.
Liczba wykonawców	1
Uwagi	

Temat pracy dyplomowej magisterskiej (jęz. pol.)	Metody pomiaru jakości dla koherentnej transmisji optycznej z bardzo dużą szybkością
Temat pracy dyplomowej magisterskiej (jęz. ang.)	Quality measurement methods for coherent optical transmission at very high speed
Opiekun pracy	Lech Smoleński
Konsultant pracy	-
Cel pracy	Ocena przydatności metod stosowanych dla pomiarów jakości transmisji w systemach optycznych wykorzystujących modulację amplitudowo-fazową i transmisję wielokanałową do

	przesyłania danych z szybkością powyżej 100 Gb/s.
Zadania do wykonania	<ol style="list-style-type: none"> 1. Przegląd metod pomiaru jakości stosowanych dla transmisji optycznej z dużymi szybkościami. 2. Ocena dokładności i łatwości realizacji poszczególnych metod pomiarowych. 3. Porównanie analizowanych metod pomiarowych i ocena ich przydatności.
Źródła	<ol style="list-style-type: none"> 1. www.lightwaveonline.com/articles/2014/11/quality-rating-of-coherent-measurements.html (05/2019) 2. Measurement of Optical Signal to Noise Ratio in Coherent Systems using Polarization Multiplexed Transmission, White Paper, www.viavisolutions.com/en-us/resources/library, (05/2019) 3. New Perspectives in Test: 400G and the new test revolution, White Paper, www.viavisolutions.com/en-us/resources/library, (05/2019)
Liczba wykonawców	1
Uwagi	

Zasady wyboru tematu:

1. Wybrany temat należy zgłosić do opiekuna i z nim przedyskutować.
2. W przypadku konfliktu wyboru decyduje średnia ocen studiów inżynierskich.
3. Po zaakceptowaniu wyboru tematu przez opiekuna należy wypełnić i podpisać kartę dyplomanta (3 egzemplarze) i złożyć w sekretariacie Katedry.