Paweł Rajba
pawel@cs.uni.wroc.pl
http://pawel.ii.uni.wroc.pl/

Seminarium: Kryptografia i bezpieczeństwo komputerowe

Organizacyjne

- Zajęcia 18:15-19:45, obecność obowiązkowa
  - Max. 2 nieobecności
- Każdy przygotuje po dwie prezentacje 35 min w dwóch seriach (do i od połowy semestru)
  - Slajdy prezentacji powinny być przygotowane w EN, natomiast językiem prezentacji jest PL.
- Kontakt: pawel@cs.uni.wroc.pl

Tematy

- Na stronie **itcourses.eu/crypto** będą tematy do wyboru
  - Pojawią się w czwartek wieczorem i potem można rezerwować przez wysłanie maila o tytule
    - [Crypto] Rezerwacja tematu
  - Do środy wieczorem można również zgłaszać własne propozycje
    - Można też później, ale można zostać wcześniej wytypowanym do tematu z listy i wtedy już nie można. Więc nie warto zwlekać
  - Do piątku wieczorem rezerwacja + ewentualna deklaracja prezentacji na 10.03
- W przypadku braku chętnego na dany termin, prezentujący będzie wyznaczany przeze mnie

Tematy

- Tematyka wstępnie
  - Homomorphic encryption
  - Post-Quantum Cryptography
  - Cryptanalysis
  - Zero Knowledge Proofs
  - Anonymity, Blind signatures
  - Proxy re-encryption schemes
  - Remote Integrity Check
  - Batch cryptography
  - Attribute/Identity based encryption, fuzzy identity based signature, multi-authority encryption schemes
  - Blockchain crypto foundations
  - TPM, HSM, TEE, SGX
  - Key management, secret sharing
  - PKI, WoT
  - Certificate Transparency

Następne zajęcia

- Zajęcia 03.03.2025 – potrzebny chętny
- Będzie łatwiej, bo:
  - Wprowadzenie w tematykę
  - Załatwia obie prezentacje
  - Do dyspozycji całe zajęcia
- Kto?
  - ???

Kryteria oceny

- [0-1] Czy na temat
- [0-1] Należy „wyrobić" się w określonym czasie
  - przewidując 3-5 minut na pytania
- [0-3] Czy treściwie i czy potencjał tematu został wykorzystany
  - W szczególności powinno się unikać „lania wody" i pustych stwierdzeń
- [0-2] Czy zrozumiale
  - Nie za łatwo ani za trudno, odpowiednie wyjaśnienia
  - Czy dostosowane do możliwości odbiorców
  - Przykłady dla omawianego zagadnienia są obowiązkowe
- [0-2] Czy ciekawie
  - Należy mówić interesująco i zaciekawić tematem
    - W szczególności nie wolno czytać ze slajdów lub je pomijać
  - Należy mówić odpowiednio głośno i wyraźnie

Kryteria oceny

- [0-2] Spójnie
  - Przedstawiony zakres powinien być spójny i kompletny
  - Poziom szczegółowości powinien być odpowiedni i kontrolowany
- [0-4] Slajdy
  - Prezentacja ma być czytelna i poprawna językowo
  - Struktura zgodna ze wzorcem:
    - Tytuł, plan, wprowadzenie, rozwinięcie, podsumowanie
  - Ma być zwięźle
    - Krótkie sformułowania, równoważniki zdań, bez „lania wody”
  - I zgodnie z innymi wytycznymi tworzenia dobrych slajdów
    - Jeśli ktoś nie ma jeszcze doświadczenia:
      - Google →
        Wyszukanie „jak zrobić dobrą prezentację”
      - Na początek warto przejrzeć to podsumowanie

Kryteria oceny

- Ocena
  - 5.0: 15-14
  - 4.5: 13-12
  - 4.0: 11-10
  - 3.5: 9-8
  - 3.0: 7-6
  - 2.0: 5-0

Typowe błędy (1/2)

- Agenda nie mapuje się na późniejsze slajdy
- Brak spójnej narracji
  - np. w połowie gubimy wątek gdzie jesteśmy i do czego zmierzamy lub też w którym punkcie agendy jesteśmy
- Brak spójności w opowieści, w strukturze
  - np. poruszane jest coś, a 3 slajdy dalej jest to samo ale inaczej
- Slajdy niedopracowane, np.
  - niespójne wypunktowania
    - np. lista z wymieszanymi pozycjami z różnych kategorii, e.g. pros/cons
  - za mała czcionka,
  - nieczytelne zrzuty ekranu,
  - niejasne sformułowania,
  - jedna opcja opisana szeroko, a druga pobieżnie

Typowe błędy (2/2)

- Suche dane bez punktu odniesienia lub punkt odniesienia mało wyraźny
- Nawiązywanie do niewyjaśnionych konceptów lub skrótów
- Za szeroki zakres prezentacji i za dużo tempo, albo odwrotnie
- Brak przykładów, lanie wody
- Mówienie za cicho, nietrzymanie się czasu
- Brak źródeł pożyczonych materiałów