Podstawy Kryptografii

LEKCJA 1 – „Nie ruszaj mojego hasła! – Hashing i Salting w praktyce”

1 | Cele lekcji

Po 45 minutach uczeń:

1. wyjaśnia, czym różni się **hash** od **szyfrowania**;
2. potrafi dodać **salt** i pokazać, jak utrudnia to atak „tęczowej tablicy”;
3. rozpoznaje, kiedy używać klucza prywatnego, a kiedy publicznego (z lotu ptaka).

2 | Czas trwania

45 min

3 | Potrzebne materiały

Co	Po co	Plan B / offline
Komputer z Linux lub WSL	polecenia sha256sum, openssl	wydruki wyników
Online tool CyberChef (browser)	szybkie mieszanie, wizualna sól	screenshoty
Kartka „Katalog haseł” (A4)	ćwiczenie do saltingu	–
Tablica / flipchart	rysunki analityczne	–

4 | Przebieg zajęć

Faza	Czas	Co robi nauczyciel	Co robią uczniowie

Hook	4'	Slajd: „admin / 123456 – znalezione w wycieku”. Pytanie: *Dlaczego takie hasło od razu pęka?*	Krótko komentują.
Hash ≠ szyfr	8'	echo -n "HELLO" | sha256sum → pokazuje jednokierunkowość. Rysuje strzałkę „tylko w prawo”.	Porównują HELLO i hello.
Tęczowa tablica	6'	Pokazuje gotowy rainbow-lookup online dla „password”.	Widzą, że hash SHA-1 jest w bazie.
Salting	15'	1️⃣ rozdaje kartki „Katalog haseł” (login, hash). 2️⃣ Każda para dodaje losowy 8-znakowy salt, łączy salt+hasło, liczy SHA-256. 3️⃣ Wspólnie próbują sprawdzić wynik w rainbow-lookup – brak!	Tworzą i testują swoje salted-hash’e.
Private / Public (zajawka)	5'	Rysunek kłódki: klucz publiczny = kłódka, prywatny = klucz w kieszeni. *Obiecujemy ciąg dalszy jutro.*	Zadają pytania.
Podsumowanie	7'	Na tablicy lista „dobrych praktyk” (unikalne hasło, salt, pieprzenie – pepper).	Fotografują notatkę; wpisują, jak wzmocniliby loginy szkolne.

5 | Pytania do dyskusji

- Czy z hasza **można** odzyskać oryginalne hasło? Dlaczego/nie?

- Jak myślisz, ile różnych hashy może istnieć dla tych samych danych? (kolizje?)

6 | Ratunkowe wskazówki

- **Brak Internetu** – użyj openssl dgst -sha256 lokalnie i wydrukowanych wyników rainbow-table.
- **Zbyt skomplikowane pytanie** – zapisz na tablicy i wróć na początku kolejnej lekcji.

7 | Dodatkowe źródła

- Cisco Packet Tracer „ACL Lab” (pliki *.pkt* do pobrania).
- Krótki film YouTube

  https://youtu.be/OBdEhSPoDaY

LEKCJA 2 – „Jak dogadać się w tajemnicy – Key Exchange, PKI i Obfuskacja”

1 | Cele lekcji

Uczeń:

1. demonstruje uproszczony **Diffie-Hellman** i tłumaczy, czemu podsłuchujący nic z tego nie ma;
2. opisuje rolę **PKI** (korzeń → CA → certyfikat) oraz podpis cyfrowy;
3. wymienia przykłady **obfuskacji** i odróżnia ją od kryptografii.

2 | Czas trwania

45 min

3 | Potrzebne materiały

Co	Funkcja
Strona https://cryptii.com/ lub własny skrypt Python „mini-DH”	interaktywne DH

openssl	generowanie pary kluczy, self-signed cert
Gotowy certyfikat szkolny (schoolCA.crt)	ćwiczenie łańcucha zaufania
Play-book „Obfuskacja vs. szyfrowanie” (A5)	analizy

4 | Przebieg zajęć

Segment	Czas	Działania nauczyciela	Rola uczniów
Rozgrzewka	3'	Przypomina kłódkę vs. klucz.	–
Diffie-Hellman „kolory farb”	12'	Slajd z mieszaniem farb: żółta (g) + sekretny niebieski (a,b) = zielony (shared).	Na kartkach stosują liczby mod 23 (g=5). Liczą wspólny sekret.
OpenSSL demo	7'	openssl genpkey -algorithm RSA -out priv.pem -pkeyopt rsa_keygen_bits:2048 → openssl rsa -pubout -in priv.pem -out pub.pem.	Oglądają nagłówek PEM; notują „BEGIN PUBLIC KEY”.
PKI łańcuch	10'	Pokazuje openssl x509 -in schoolCA.crt -text -noout. Koloryzuje: *Issuer*, *Subject*, *Signature*. Rysuje piramidę CA.	Łączą strzałkami: root → intermediate → cert serwera.
Obfuskacja ≠ szyfr	6'	CyberChef: Rot-13 i Base64 („ZWxv...”) → łatwe odwrócenie. Podkreśla, że to ukrywanie, a nie ochrona.	Próbują „zaszyfrować” imię Base64 i *odkryć*, że to nie szyfr.

Ćwiczenie grupowe	5'	Każdej grupie rozdaje wycinek loga TLS. Zadanie: zaznacz miejsce handshake, certyfikatu i key exchange.	Kolorują plik, prezentują.
Podsumowanie	2'	Lista na tablicy: *hash – jednokierunkowy, key exchange – tajny kanał, PKI – zaufanie publiczne, obfuskacja – kosmetyka*.	Self-check: dopasowują definicję → słowo.

5 | Pytania do dyskusji

- Dlaczego w Diffie-Hellman nie przesyłamy klucza wprost?
- Po co nam jeszcze certyfikat, skoro mamy już klucz publiczny serwera?
- W jakiej sytuacji obfuskacja **wystarcza**, a kryptografia byłaby przesadą?

6 | Ratunkowe wskazówki

- **Matematyka DH przerasta grupę** – wróć do analogii z farbami i nie wchodź w moduły > 30. Istotna jest idea wspólnej tajemnicy, nie liczby pierwsze.
- **Brak OpenSSL na komputerach** – pokaż wynik wideo / zrzuty per krok, uczniowie opisują, co się dzieje.

7 | Dodatkowe źródła

- Film na Youtube https://youtu.be/NmM9HA2MQGI