**Lekcja 4**

**Temat: Chrońmy informacje, czyli techniki uwierzytelniania, kryptografia.**

**Uwierzytelnianie** - stwierdzenie autentyczności dokumentu lub podpisu.

**Proces uwierzytelniania**

**1. Identyfikacja**

Podczas identyfikacji jest sprawdzana nasza tożsamość.

- aby zalogować się na pocztę elektroniczną czy do konta w mediach społecznościowych, podajemy login, który następnie jest weryfikowany w bazie danych

- jeżeli chcemy uzyskać informacje dotyczące naszego konta na infolinii banku, zostaniemy poproszeni o podanie naszego imienia i nazwiska

**2. Uwierzytelnianie**

Jest to moment kiedy strona ufająca za pomocą dostępnych sobie narzędzi i metod weryfikuje, czy dany użytkownik jest tym za kogo się podaje

- serwer na którym mamy swoją skrzynkę pocztową prosi nas o wpisanie hasła

- obsługa banku zadaje kolejne pytania, które pomogą w weryfikacji naszej tożsamości, np. data urodzenia, pesel, nazwisko panieńskie matki

**3. Autoryzacja**

W tym kroku otrzymamy prawo lub odmowę dostępu do danych

**Techniki uwierzytelniania**

**-**  w przypadku dokumentów pisanych

W przypadku dokumentów pisanych, np. pieczęć instytucji, podpis osoby uprawnionej, znak wodny

- w przypadku osób lub istot żywych techniką uwierzytelniania jest zabezpieczenie biometryczne (Rozpoznanie tęczówki oka, linie papilarne, geometria dłoni), karta elektroniczna, bioczip i token

- w przypadku dokumentów i wiadomości elektronicznych technikami uwierzytelniania są podpis cyfrowy, kod uwierzytelnienia wiadomości

- w przypadku komunikacji elektronicznej stosuje się techniki oparte na kryptografii symetrycznej lub niesymetrycznej lub haśle jednorazowym

**Kodowanie** – ustalone słowa, wyrażenia lub symbole stosowane raz w ogólnodostępnym przekazie

„Agata zaczęła rodzić - może informować o podłożonym ładunku wybuchowym”

**Szyfrowanie** – odbywa się na poziomie pojedynczych znaków, np. szyfrowanie cezara

**Podpis elektroniczny** – jest operacją podpisywania konkretnych danych przez osobę fizyczną

**Podpis cyfrowy** – jest to zbiór danych dołączony do innych danych, które pozwala odbiorcy danych udowodnić pochodzenie danych i zabezpieczyć je przed fałszerstwem