### Zadanie 2: Podstawowe atrybuty kryptograficznej ochrony informacji to: (☑️ Oryginalna | ✅ Poprawna | ❌ Niepoprawna)

* ☑️ ✅ **uwierzytelnienie**
* ☑️ ✅ **integralność**
* ☑️ ✅ **poufność**
* ❌ **dostępność**

**Ocena:** **Poprawnie.** Dostępność, choć jest ważnym elementem bezpieczeństwa IT, nie jest zaliczana do podstawowych *kryptograficznych* atrybutów ochrony informacji omawianych na wykładzie.

### Zadanie 3: Kryptograficzna usługa uwierzytelnienia ma na celu: (☑️ Oryginalna | ✅ Poprawna | ❌ Niepoprawna)

* ☑️ ✅ **potwierdzenie tożsamości danej strony protokołu kryptograficznego**
* ❌ **zapewnienie dostępności danych**
* ❌ **zweryfikowanie poprawności danych (czy nie zostały zmodyfikowane)** – To jest cel usługi **integralności**.
* ❌ **ochronę danych przed ich ujawnieniem** – To jest cel usługi **poufności**.

**Ocena:** **Poprawnie.**

### Zadanie 4: Kryptograficzna usługa integralności ma na celu: (☑️ Oryginalna | ✅ Poprawna | ❌ Niepoprawna)

* ❌ **ochronę danych przed ich ujawnieniem** – Cel **poufności**.
* ❌ **potwierdzenie tożsamości danej strony protokołu kryptograficznego** – Cel **uwierzytelnienia**.
* ☑️ ✅ **zweryfikowanie poprawności danych (czy nie zostały zmodyfikowane)**
* ❌ **zapewnienie dostępności danych**

**Ocena:** **Poprawnie.**

### Zadanie 5: Kryptograficzna usługa poufności ma na celu: (☑️ Oryginalna | ✅ Poprawna | ❌ Niepoprawna)

* ❌ **zweryfikowanie poprawności danych (czy nie zostały zmodyfikowane)** – Cel **integralności**.
* ❌ **zapewnienie dostępności danych**
* ☑️ ✅ **ochronę danych przed ich ujawnieniem**
* ❌ **potwierdzenie tożsamości danej strony protokołu kryptograficznego** – Cel **uwierzytelnienia**.

**Ocena:** **Poprawnie.**

### Zadanie 6: System kryptograficzny zapewniający poufność informacji musi spełniać następujące warunki: (☑️ Oryginalna | ✅ Poprawna | ❌ Niepoprawna)

* ☑️ ✅ **nie może zawierać mechanizmów pozwalających na odczyt informacji przez nieuprawnione strony protokołu kryptograficznego, tzw. tylne furtki (back doors)**
* ☑️ ✅ **przekształcenia szyfrujące i deszyfrujące muszą być efektywne dla wszystkich kluczy**
* ❌ **może zawierać mechanizmy pozwalające na odczyt informacji przez nieuprawnione strony...**
* ☑️ ✅ **przekształcenia szyfrujące i deszyfrujące muszą być wzajemnie odwrotne**

**Ocena:** **Poprawnie.** Zaznaczone odpowiedzi są zgodne z podstawowymi własnościami kryptosystemu opisanymi w transkrypcji.

### Zadanie 7: Zasada Kerckhoffsa stwierdza, że: (☑️ Oryginalna | ✅ Poprawna | ❌ Niepoprawna)

* ❌ **bezpieczeństwo kryptosystemu powinno być oparte na tajności odpowiednich kluczy kryptograficznych oraz zależeć od tajności algorytmów kryptograficznych**
* ❌ **bezpieczeństwo kryptosystemu powinno być oparte na jawności wszystkich kluczy...**
* ☑️ ✅ **bezpieczeństwo kryptosystemu powinno być oparte na tajności odpowiednich kluczy kryptograficznych i nie zależeć od tajności algorytmów kryptograficznych**
* ❌ **bezpieczeństwo kryptosystemu powinno być oparte na jawności wszystkich kluczy...**

**Ocena:** **Poprawnie.** Jest to dokładna definicja zasady Kerckhoffsa podana w transkrypcji.

### Zadanie 8: W kryptografii symetrycznej: (☑️ Oryginalna | ✅ Poprawna | ❌ Niepoprawna)

* ✅ **w procesie szyfrowania deszyfrowania wykorzystują szyfry blokowe i/lub strumieniowe**
* ☑️ ✅ **w procesie szyfrowania/deszyfrowania używany jest ten sam klucz kryptograficzny** (lub klucze łatwe do wzajemnego wyliczenia)
* ❌ **zapewniają uwierzytelnienie poprzez generację/weryfikację podpisu cyfrowego** – To domena kryptografii asymetrycznej.
* ❌ **każda ze stron protokołu kryptograficznego posiada 2 różne klucze: publiczny (jawny) oraz prywatny (tajny)** – To cecha kryptografii asymetrycznej.

**Ocena:** **Częściowo poprawnie.** Zaznaczona odpowiedź jest prawidłowa, ale pierwsza odpowiedź również jest poprawna. Szyfry blokowe i strumieniowe to dwie główne kategorie szyfrów symetrycznych omawiane na wykładach.

### Zadanie 9: W kryptografii symetrycznej klucze powinny spełniać następujące warunki: (☑️ Oryginalna | ✅ Poprawna | ❌ Niepoprawna)

* ❌ **klucz deszyfrowania może być jawny...**
* ❌ **klucz szyfrowania/deszyfrowania może być jawny**
* ☑️ ✅ **klucz szyfrowania/deszyfrowania musi być tajny**
* ❌ **klucz szyfrowania może być jawny...**

**Ocena:** **Poprawnie.** W kryptografii symetrycznej tajność klucza jest absolutnie fundamentalna.

### Zadanie 10: Szyfry strumieniowe: (☑️ Oryginalna | ✅ Poprawna | ❌ Niepoprawna)

* ☑️ ✅ **przekształcają strumień bitów tekstu jawnego w strumień bitów tekstu zaszyfrowanego za pomocą strumienia bitów tajnego klucza symetrycznego**
* ❌ **przekształcają bloki tekstu jawnego w bloki tekstu zaszyfrowanego...** – To definicja szyfrów blokowych.
* ❌ **stanowią klasę kryptosystemów asymetrycznych**
* ☑️ ✅ **stanowią klasę kryptosystemów symetrycznych**

**Ocena:** **Poprawnie.**

### Zadanie 11: Szyfry blokowe: (☑️ Oryginalna | ✅ Poprawna | ❌ Niepoprawna)

* ☑️ ✅ **stanowią klasę kryptosystemów symetrycznych**
* ❌ **stanowią klasę kryptosystemów asymetrycznych**
* ☑️ ✅ **przekształcają bloki tekstu jawnego w bloki tekstu zaszyfrowanego za pomocą tajnego klucza symetrycznego**
* ❌ **przekształcają bloki tekstu jawnego w bloki tekstu zaszyfrowanego za pomocą jawnego klucza asymetrycznego**

**Ocena:** **Poprawnie.**

### Zadanie 12: Kryptograficzna funkcja skrótu: (☑️ Oryginalna | ✅ Poprawna | ❌ Niepoprawna)

* ☑️ ✅ **przekształca ciąg binarny o dowolnej, skończonej długości w wektor binarny o określonej długości**
* ☑️ ✅ **służy do realizacji usługi integralności informacji**
* ❌ **służy do realizacji usługi poufności informacji**
* ❌ **przekształca ciąg binarny o określonej długości w ciąg bitów o tej samej długości**

**Ocena:** **Poprawnie.**

### Zadanie 13: Współczesne szyfry blokowe mogą być projektowane w oparciu o: (☑️ Oryginalna | ✅ Poprawna | ❌ Niepoprawna)

* ❌ **strukturę iteracyjną Merklego-Damgarda MD** – To konstrukcja funkcji skrótu.
* ❌ **rejestry z liniowym sprzężeniem zwrotnym LFSR** – To budulec szyfrów strumieniowych.
* ☑️ ✅ **architekturę sieci Feistela**
* ☑️ ✅ **architekturę sieci podstawieniowo-przestawieniowej SPN**

**Ocena:** **Poprawnie.**

### Zadanie 14: Współczesne szyfry strumieniowe mogą być projektowane w oparciu o: (☑️ Oryginalna | ✅ Poprawna | ❌ Niepoprawna)

* ❌ **architekturę sieci podstawieniowo-przestawieniowej SPN** – Architektura szyfrów blokowych.
* ❌ **architekturę Feistela** – Architektura szyfrów blokowych.
* ☑️ ✅ **nieliniowe rejestry ze sprzężeniem zwrotnym NFSR**
* ☑️ ✅ **liniowe rejestry ze sprzężeniem zwrotnym LFSR**

**Ocena:** **Poprawnie.**

### Zadanie 15: Funkcja skrótu może być zbudowana w oparciu o strukturę: (☑️ Oryginalna | ✅ Poprawna | ❌ Niepoprawna)

* ❌ **LFSR** – Budulec szyfrów strumieniowych.
* ☑️ ✅ **Merkle-Damgarda**
* ☑️ ✅ **gąbki**
* ❌ **sieć Feistela** – Architektura szyfrów blokowych.

**Ocena:** **Poprawnie.**

### Zadanie 16: AES: (☑️ Oryginalna | ✅ Poprawna | ❌ Niepoprawna)

* ☑️ ✅ **zastosowano konstrukcję sieci podstawieniowo-przestawieniowej SPN**
* ❌ **zastosowano konstrukcję sieci Feistela**
* ☑️ ✅ **jest standardem szyfrowania blokowego**
* ☑️ ✅ **długość klucza wynosi 128, 192 lub 256 bitów**

**Ocena:** **Poprawnie.**

### Zadanie 17: Funkcja skrótu SHA-3: (☑️ Oryginalna | ✅ Poprawna | ❌ Niepoprawna)

* ☑️ ✅ **daje skrót o długości 224, 256, 384 lub 512 bitów**
* ☑️ ✅ **jest standardem funkcji skrótu**
* ❌ **zbudowana jest w oparciu o konstrukcję Merkle-Damgarda (MD)** – Na tej konstrukcji oparto SHA-1 i SHA-2.
* ☑️ ✅ **zbudowana jest w oparciu o architekturę "gąbki" (sponge construction)**

**Ocena:** **Poprawnie.**

### Zadanie 18: W kryptografii asymetrycznej: (☑️ Oryginalna | ✅ Poprawna | ❌ Niepoprawna)

* ❌ **klucze asymetryczne publiczny i prywatny są wygenerowane losowo i nie zależą od siebie**
* ☑️ ✅ **klucze asymetryczne publiczny i prywatny są wygenerowane z wykorzystaniem problemu trudno obliczeniowego i są wzajemnie zależne**
* ☑️ ✅ **każda strona protokołu kryptograficznego posiada parę kluczy asymetrycznych: publiczny (jawny) i prywatny (tajny)**
* ❌ **każda strona protokołu kryptograficznego posiada wspólny klucz tajny** – To cecha kryptografii symetrycznej.

**Ocena:** **Poprawnie.**

### Zadanie 19: Kryptosystemy asymetryczne: (☑️ Oryginalna | ✅ Poprawna | ❌ Niepoprawna)

* ☑️ ✅ **są warunkowo bezpieczne**
* ☑️ ✅ **bezpieczeństwo oparte jest na problemie trudno obliczeniowym**
* ☑️ ✅ **bezpieczeństwo zależy od aktualnej wiedzy i możliwości technologicznych dot. rozwiązywania danego problemu trudnoobliczeniowego**
* ❌ **są bezwarunkowo bezpieczne** – Bezwarunkowo bezpieczny jest np. szyfr z kluczem jednorazowym (One-Time Pad).

**Ocena:** **Poprawnie.**

### Zadanie 20: Protokół Diffie-Hellmana służy do: (☑️ Oryginalna | ✅ Poprawna | ❌ Niepoprawna)

* ❌ **szyfrowania/deszyfrowania wiadomości**
* ☑️ ✅ **ustalenia wspólnej, tajnej wartości, która może służyć do generacji klucza symetrycznego przez strony protokołu kryptograficznego**
* ❌ **uwierzytelniania wiadomości**
* ❌ **generacji/weryfikacji podpisu cyfrowego wiadomości**

**Ocena:** **Poprawnie.**

### Zadanie 21: Odbiorca otrzymał od Nadawcy wiadomość podpisaną cyfrowo [...]. Którego klucza użyje Odbiorca w procesie weryfikacji [...]? (☑️ Oryginalna | ✅ Poprawna | ❌ Niepoprawna)

* ❌ **klucza publicznego Odbiorcy**
* ❌ **klucza prywatnego Nadawcy**
* ❌ **klucza prywatnego Odbiorcy**
* ☑️ ✅ **klucza publicznego Nadawcy**

**Ocena:** **Poprawnie.**

### Zadanie 22: Odbiorca otrzymał od Nadawcy wiadomość zaszyfrowaną [...]. Którego klucza użyje Odbiorca w procesie deszyfrowania? (☑️ Oryginalna | ✅ Poprawna | ❌ Niepoprawna)

* ❌ **klucza publicznego Odbiorcy**
* ☑️ ✅ **klucza prywatnego Odbiorcy**
* ❌ **klucza prywatnego Nadawcy**
* ❌ **klucza publicznego Nadawcy**

**Ocena:** **Poprawnie.**

### Zadanie 23: W kryptografii asymetrycznej, w przypadku wiadomości nadawanej przez Nadawcę i odbieranej przez Odbiorcę: (☑️ Oryginalna | ✅ Poprawna | ❌ Niepoprawna)

* ☑️ ✅ **w realizacji usługi poufności wiadomości klucz publiczny Odbiorcy służy do szyfrowania wiadomości przez nadawcę, a klucz prywatny Odbiorcy do jej deszyfrowania przez odbiorcę**
* ❌ **w realizacji usługi poufności wiadomości, klucz prywatny Nadawcy służy do szyfrowania...**
* ☑️ ✅ **w realizacji usługi uwierzytelnienia nadawcy klucz prywatny Nadawcy służy do generacji podpisu cyfrowego a klucz publiczny Nadawcy do jego weryfikacji przez odbiorcę**
* ❌ **w realizacji usługi uwierzytelnienia nadawcy klucz publiczny Odbiorcy służy do generacji podpisu...**

**Ocena:** **Poprawnie.**

### Zadanie 24: Kryptosystem ElGamala może służyć do: (☑️ Oryginalna | ✅ Poprawna | ❌ Niepoprawna)

* ☑️ ✅ **generacji/weryfikacji podpisu cyfrowego wiadomości**
* ☑️ ✅ **szyfrowania/deszyfrowania wiadomości**
* ❌ **zapewnienia dostępności do wiadomości**
* ❌ **zapewnienia integralności wiadomości** – Integralność jest *skutkiem ubocznym* weryfikacji podpisu, ale nie jest to główna usługa realizowana bezpośrednio przez algorytm w taki sposób, jak poufność czy uwierzytelnienie.

**Ocena:** **Poprawnie.** Zgodnie z transkrypcją, ElGamal jest przedstawiony obok RSA jako system do szyfrowania i podpisywania.

### Zadanie 25: Problemem trudno obliczeniowym dla RSA jest: (☑️ Oryginalna | ✅ Poprawna | ❌ Niepoprawna)

* ❌ **problem obliczania logarytmu dyskretnego...**
* ❌ **problem obliczania logarytmu dyskretnego na krzywych eliptycznych**
* ☑️ ✅ **problem faktoryzacji (rozkład liczby złożonej na czynniki pierwsze)**
* ❌ **problem plecakowy**

**Ocena:** **Poprawnie.**

### Zadanie 26: Problemem trudno obliczeniowym dla algorytmu ElGamala jest: (☑️ Oryginalna | ✅ Poprawna | ❌ Niepoprawna)

* ❌ **problem obliczania logarytmu dyskretnego na krzywych eliptycznych** – To podstawa kryptografii krzywych eliptycznych (ECC), która jest osobną dziedziną.
* ☑️ ✅ **problem obliczania logarytmu dyskretnego w ciele liczb całkowitych modulo duża liczba pierwsza**
* ❌ **problem plecakowy**
* ❌ **problem faktoryzacji (rozkład liczby złożonej na czynniki pierwsze)** – To problem dla RSA.

**Ocena:** **Poprawnie.**

### Zadanie 27: Obecnie, minimalna (rekomendowana przez NIST) długość klucza ElGamala wynosi: (☑️ Oryginalna | ✅ Poprawna | ❌ Niepoprawna)

* ❌ **512 bitów**
* ❌ **1024 bity**
* ☑️ ✅ **2048 bitów**
* ❌ **4096 bitów**

**Ocena:** **Poprawnie.** Wykładowca wspomina o rekomendacji NIST wynoszącej 2048 bitów dla algorytmów opartych na logarytmie dyskretnym.

### Zadanie 28: Obecnie minimalna (wg NIST) długość liczby pierwszej w protokole Diffie-Hellmana [...] wynosi: (☑️ Oryginalna | ✅ Poprawna | ❌ Niepoprawna)

* ❌ **512 bitów**
* ❌ **1024 bity**
* ☑️ ✅ **2048 bitów**
* ❌ **4096 bitów**

**Ocena:** **Poprawnie.** To samo zalecenie NIST dotyczy protokołu Diffie-Hellmana.

### Zadanie 29: Które z poniższych sformułowań jest prawdziwe? (☑️ Oryginalna | ✅ Poprawna | ❌ Niepoprawna)

* ☑️ ✅ **kryptoanaliza to dziedzina wiedzy i badań zajmująca się analizowaniem (łamaniem) istniejących algorytmów kryptograficznych**
* ☑️ ❌ **kryptologia zajmuje się ukrywaniem informacji**
* ☑️ ✅ **kryptologia to nauka obejmująca kryptografię i kryptoanalizę**
* ☑️ ✅ **kryptografia to dziedzina wiedzy i badań zajmująca się tworzeniem nowych algorytmów kryptograficznych**

**Ocena:** **Częściowo poprawnie.** Trzy z czterech zaznaczonych odpowiedzi są w pełni poprawne. Odpowiedź "kryptologia zajmuje się ukrywaniem informacji" jest nieprecyzyjna. Wykładowca wyraźnie rozróżnia kryptografię (która sprawia, że informacja jest nieczytelna) od steganografii (która zajmuje się *ukrywaniem* faktu istnienia informacji).

### Zadanie 30: Nadawca chce wysłać do Odbiorcy wiadomość podpisaną cyfrowo. Którego klucza użyje Nadawca w procesie generacji podpisu cyfrowego? (☑️ Oryginalna | ✅ Poprawna | ❌ Niepoprawna)

* ❌ **klucza publicznego Odbiorcy**
* ❌ **klucza publicznego Nadawcy**
* ❌ **klucza prywatnego Odbiorcy**
* ☑️ ✅ **klucza prywatnego Nadawcy**

**Ocena:** **Poprawnie.**