CYBER SECURITY

1. forduló

Continental
The Future in Motion

A kategória támogatója: Continental

RENDELKEZÉSRE ÁLLÓ IDŐ:

25:00

Ismertető a feladathoz

Fontos információk:

A kérdésekre **mindig van helyes válasz**! Ha csak egy helyes válasz van az adott kérdésre, radio button-os választási lehetőségeket fogsz látni.

Kérjük, hogy a feladatok szövegeit **ne másold** és a böngésződ fejlesztő eszközét/ konzolját se nyisd meg feladatmegoldás közben! Mindkettő kizárást vonhat maga után.

Minden forduló után a **megoldások csütörtök reggel 8 órakor** lesznek elérhetőek.

A megoldásokkal kapcsolatos esetleges **észrevételeket a megoldások megjelenését követő kedd éjfélig** várjuk.

A több válaszlehetőségű feleletválasztós kérdéseknél járnak **részpontszámok, ha egyik rossz választ sem jelölöd be**.

Ha kifutsz az adott feladatlap kitöltésére rendelkezésre álló időből, a felület **automatikusan megpróbálja beküldeni** az addig megadott válaszokat.

Minden feladatsornak van egy **becsült minimum megoldási ideje** (legalább a feladat elolvasási ideje). Aki ennél rövidebb idő alatt oldja meg, kizárható a versenyből.

Az első kategória után, amelynek a feladatlapját megoldod a fordulóban, kapni fogsz egy 2-3 perc alatt kitölthető **kérdőívet**. Az ezekből összeállított piackutatás legfontosabb eredményeit a díjátadót követően Veled is megosztjuk majd. Formáljuk közösen a piacot!

Első forduló

Ahhoz, hogy tisztában legyünk a Cyber Security és a kriptográfia alapjaival, fontos, hogy az alapokat ismerjük.

Az első 3 fordulóban jobbára a témához kapcsolódó elméleti kérdésekkel találkozhatsz, majd érkeznek a gyakorlatiasabb és komplexebb feladatok.

Felhasznált idő: 02:03/25:00 **Elért pontszám:** 0/12

1. feladat 0/0 pont

A titkosítás olyan eljárás, amely az információt olyan formává alakítja, amit csak a célszemély tud értelmezni.

Válasz

- ◯ Igaz
- ◯ Hamis

Magyarázat

2. feladat 0/1 pont

A szimmetrikus titkosításhoz több, különböző kulcsot használnak.

Válasz

- ◯ Igaz
- ◯ Hamis

Magyarázat

3. feladat 0/1 pont

A digitális aláíráshoz aszimmetrikus titkosítást használunk.

Válasz

- ◯ Igaz
- ◯ Hamis

Magyarázat

4. feladat 0/0 pont

Az aszimmetrikus kulcsú titkosítás esetén a titkos kulcs előállítható a nyilvános kulcs ismeretében.

Válasz

- ○ Igaz
- ◯ Hamis

Magyarázat

Frissítés (2021.11.24.): mindkét válasz mellett lehet érvelni a versenyzői visszajelzések alapján, ezért a kérdést 0 pontosra állítottuk

5. feladat 0/1 pont

Az alábbiak közül melyik nem szimmetrikus titkosítás?

Válasz

- ○ DES
- ○ AED
- ◯ RSA
- ○ IDEA

Magyarázat

6. feladat 0/1 pont

Fejtsd meg az alábbi titkosított szöveget!

GSRXMRIRXEPVYPIW

Segítség: az eljárás szimmetrikus és már az ókorban ismerték és használták.

Válaszok

A helyes válasz:
CONTINENTALRULES
Caesar kódolás, 4-es eltolás, a dekódolt információ: ContinentalRules
continental rules

Magyarázat

7. feladat 0/1 pont

Az alábbiak közül melyik a rejtjelezéssel, titkosírással, kódolással foglalkozó tudományág?

Válasz

- calligráfia
- diszgráfia
- kriptográfia
- szteganográfia

Magyarázat

8. feladat 0/1 pont

Mi az elektronikus aláírás gyakorlati lényege?

Válasz

- Az üzenet sértetlenségének, küldés időpontjának a hitelesítése és az üzenet címzettjének azonosítása.
- Az üzenet sértetlenségének, küldés időpontjának a hitelesítése és a küldő egyértelmű azonosítása.
- Az üzenet sértetlenségének, küldés időpontjának a hitelesítése és a küldő személyének elrejtése.
- Az üzenet tartalmának és küldés időpontjának a kódolása és a küldő személyének azonosítása.
- Az üzenet tartalmának és küldés időpontjának a hitelesítése és a küldő személyének azonosítása.

Magyarázat

9. feladat 0/1 pont

Egy modern kriptográfiai algoritmus biztonsága függ a(z) ...

Válasz

- titkosítandó üzenet hosszától.
- titkosítandó üzenet tartalmától.
- az üzenetküldéshez használt csatornától.
- a titkosító kulcs hosszától.

Magyarázat

10. feladat 0/1 pont

Jelöld az egyetlen helyes választ!

Információbiztonsági szempontból tekintve az aktív támadó ...

Válasz

- lehallgatja és továbbítja az üzenetet
- lehallgatja, megfejti és továbbítja az üzenetet
- lehallgatja és megsemmisíti az üzenetet
- lehallgatja és megváltoztatva tovább küldi az eredeti címzettnek az üzenetet

Magyarázat

11. feladat 0/1 pont

Amennyiben a titkosításra szolgáló kulcs nyilvánosságra kerül, ...

Válasz

- ○ a titkosító algoritmust le kell cserélni.
- ○ a titkosító algoritmust és a kulcsot le kell cserélni.
- ○ a kulcs titkosságáért felelős rendszereket le kell cserélni.
- ◯ a kulcsot le kell cserélni.

Magyarázat

12. feladat 0/1 pont

Az alábbiak közül mely csatornák, interfész(ek) tekinthetők lehetséges támadási felületnek, melyen keresztül a gépjármű informatikai rendszere támadható és szükséges az(ok) védelméről gondoskodni?

Válaszok

- ☑ Bluetooth kapcsolat
- ☑ Gépjármű kommunikációs hálózata (CAN,. LIN)
- ☑ Diagnosztika (OBD2)
- ☑ Felhő alapú SW frissítést támogató rendszerek
- ☐ Car TDUx system

Magyarázat

13. feladat 0/1 pont

Melyik a kakukktojás?

Válasz

- ○ Nyilvános kulcs
- ○ Titkos kulcs
- ○ Moduláris számelmélet

- ◯ Fibonacci számok

Magyarázat

14. feladat 0/1 pont

Igaz-e, hogy a seed-key titkosítási módszer aszimmetrikus?

Válasz

- ◯ Igaz
- ◯ Hamis

Magyarázat