Test z odborného základu navazujícího magisterského studijního programu Technologie pro obranu a bezpečnost – studijní obor Technologie pro ochranu majetku a osob.

AR 2019/2020

Identifikační číslo:

Počet bodů	Hodnocení

Počet otázek: 10
Čas: 60 minut
Bodové hodnocení otázek:

Č. otázky	Body
1	10
2	10
3	10
4	10
5	10
6	10
7	10
8	10
9	10
10	10

OTÁZKY:

1) Jak se dělí kmitočtové filtry podle amplitudové frekven+ční charakteristiky?
2) principech jsou založeny autentizační metody.
3) Uveďte hlavní důvod použití duálních pohybových čidel. Jaká je nejvhodnější kombinace duálních pohybových čidel?
4) K čemu slouží bezpečnostní deskriptor (security descriptor) v operačním systému MS Windows?
5) Nakreslete a popište schéma komunikačního řetězce (Shannonovo schéma).
6) Znázorněte Feistelovo schéma jako stavební prvek šifrovacího standardu 3DES a vysvětlete pojmy: Lavinovitost, Bezkoliznost, Konfuze a Difuze.
7) Jaké jsou hlavní bezpečnostní systémy pneumatik a jejich funkce.
8) Jaké jsou hlavní prvky vnější pasivní bezpečnosti vozidla.
9) Jak je definována účinnost systému fyzické ochrany.
10) Vysvětlete pojmy nežádoucí a falešný poplach

AUTORSKÉ ŘEŠENÍ

Otázka č. 1

Kmitočtové filtry se podle amplitudové frekvenční charakteristiky dělí na: dolní propust (DP), horní propust (HP), pásmovou propust (PP) a pásmovou zádrž (PZ).

Otázka č. 2

Autentizační metody jsou založeny na následujících základních principech:

- na základě toho, že uživatel něco zná (např. heslo),
- na základě toho, že uživatel něco vlastní (např. čipovou kartu),
- na základě biometrických vlastností (např. otisky prstů).

Otázka č. 3

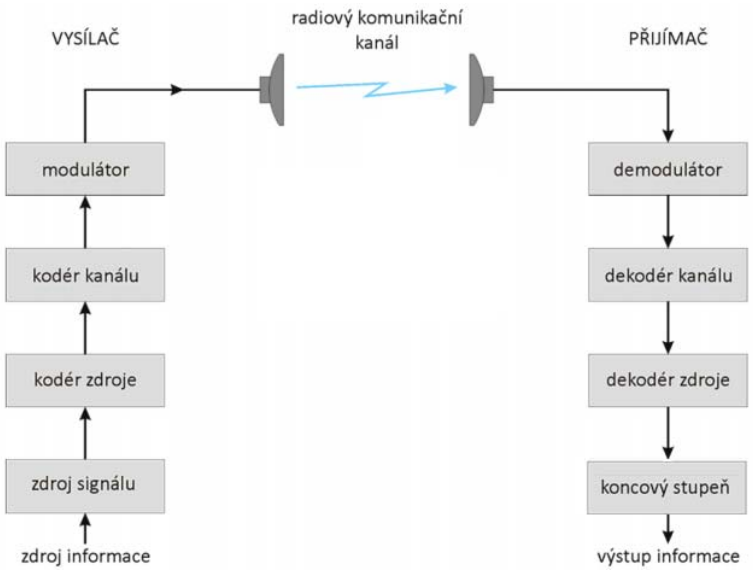
Je zanedbatelná pravděpodobnost jevů, které by u 2 čidel pracujících na různých fyzikálních principech, vyvolaly nežádoucí signalizaci současně. Tedy hlavní důvod použití duálních pohybových čidel je výrazné omezení nežádoucích poplachů. Nejvhodnější kombinace duálních pohybových čidel je pasivní infračervená čidla s mikrovlnnými čidly (PIR-MW).

Otázka č. 4

Bezpečnostní deskriptor je datová struktura spojená s objekty jako je soubor, adresář, položka registru nebo objekt v aktivním adresáři. Obsahuje mimo jiné dva seznamy přístupových práv - DACL a SACL, a informaci o vlastníkovi objektu. DACL (Discretionary Access Control List) řídí přístup uživatelů k objektu, SACL (System Access Control List) umožňuje sledovat a zaznamenávat přístupy uživatelů k objektu.

Vlastníkem objektu je typicky ten uživatel, který objekt vytvořil. Vlastník objektu může modifikovat obsah bezpečnostního deskriptoru.

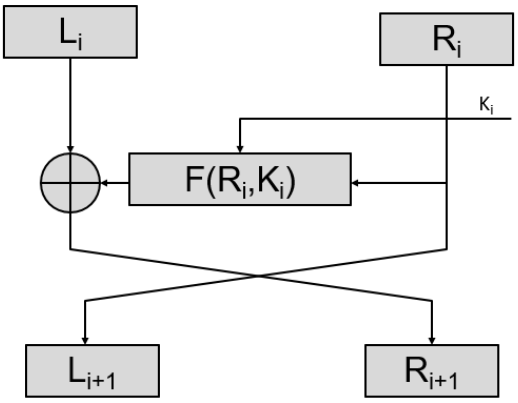
Otázka č. 5



Zdroj signálu – přeměna přenášené informace na elektrický signál. Zdrojem signálu může být např. mikrofon či televizní snímací elektronka.
Kodér zdroje – digitalizace signálu. Hlavním úkolem je ovšem odstranění redundance a irelevance. Zatímco irelevance představuje „zbytečnou“ složku, redundance by se dala definovat jako jakási nadbytečnost. Proces zdrojového kódování lze výstižně označit také jako kompresi dat. Irelevantní složka je při kompresi odstraněna nenávratně, redundantní složka je po přenosu při dekompresi obnovována, pro plnohodnotné zobrazení informace je nepostradatelná (***dekodér zdroje***).
Kodér kanálu – zatímco kodér zdroje odstraňuje irelevantní a redundantní složku signálu, čímž zmenšuje přenosovou rychlost signálu, kodér kanálu provádí operaci (kanálové kódování), při které je naopak k signálu určitá redundantní složka přidávána. Redundantní složka, kterou při kanálovém kódování k signálu přidáme, není náhodná, ale přesně kontrolovaná. Algoritmy provádějící inverzní operaci (kanálové dekódování) v ***dekodéru kanálu*** tak díky znalosti závislostí této „kontrolované“ redundantní složky umožní získat požadovanou informaci i ze signálu, který je degradován působením šumu a interferencí. Zařazení kodéru/dekodéru kanálu tak umožní snížení vysílacích výkonů, ke správnému přijetí informace totiž postačí „nižší kvalita“ signálu.
Modulátor – v modulátoru dochází k „modulování“ informačního signálu na vysokofrekvenční či mikrovlnnou nosnou vlnu. Modulaci můžeme obecně definovat jako proces, při kterém se některý z parametrů nosné vlny mění v rytmu modulačního signálu. Modulace umožňuje přesun signálu do požadovaného frekvenčního pásma, čímž je umožněno např. rozdělení kmitočtového spektra mezi jednotlivé systémy.

Otázka č. 6

Feistelovo schéma



Lavinovitost – jeden změněný bit vstupního bloku zprávy změní svojí hodnotou polovinu bitů výstupního bloku kryptogramu *(minimální změna vstupu vyvolá maximální změnu výstupních bitů)*
Bezkoliznost – neexistence korelace mezi OT a ŠT (zprávou a kryptogramem) ani ŠT a K *(kryptogramem a šifrovacím klíčem) nebo (jedním ze vstupů a výstupem)*. Není možné najít univerzální vztah mezi klíčem, algoritmem a zprávou. *(zaručuje neprolomitelnost).*
Konfuze – vztah mezi klíčem a šifrovým textem není zřejmý. Dosahováno pomocí substituce *(s boxů) (substitučních boxů)* v DES, 3DES i v AES.
Difuze – vliv každého bitu otevřeného textu na několik *(mnoho, ideálně polovinu)* bitů šifrového textu s cílem zakrýt statistické vlastnosti otevřeného textu. Difuzním prvkem je použití bitové permutace *(permutační funkce)* u DES.

Otázka č. 7

Bezpečnostní ráfky – jsou opatřením, které brání sesmeknutí pneumatiky při nadměrném snížení, nebo úplném úniku tlaku vzduchu v pneumatice. Jejich podstatou je vytvoření vhodného tvaru okraje ráfku.
Pneumatiky pro nouzový dojezd – používají technologie, které brání úniku vzduchu z pneumatiky při defektu, nebo zabrání destrukci pneumatiky a umožní dojezd vozidla na omezenou vzdálenost.
Monitorovací systémy pneumatik – přímý měřící systém s čidlem v pneumatikách a nepřímý systém využívající signály ABS.

Otázka č. 8

Mezi hlavní prvky zajišťující vnější pasivní bezpečnost vozidel patří:

- tvar přední části karoserie,
- deformační vlastnosti přední části karoserie – aktivní kapota,
- bezpečnostní (aktivní) nárazníky,
- tvary vyčnívajících částí – klik, zrcátek a stěračů,
- použití vnějších airbagů.

Otázka č. 9

Účinnost systému fyzické ochrany – charakterizuje schopnost systému fyzické ochrany zabránit negativnímu působení dané hrozby na chráněný zájem. Je definována jako součin pravděpodobnosti přerušeni útoku P_I a pravděpodobnosti neutralizace útoku P_N ostrahou objektu:

$P_E = P_I \ P_N$

Otázka č. 10

Nežádoucí poplach - poplach bez přítomnosti nebezpečí pro chráněný zájem. Je v rámci standardní činnosti systému vyvolán jinou příčinou než aktivitou narušitele. Např. chybou obsluhy (vstup do střeženého prostoru při zapnutém systému), působením vlivů prostředí (tepelné sálání, vítr, průvan …), pohybem zvířat apod. Senzor reaguje na fyzikální změny související s podstatou jeho činnosti.

Falešný poplach - *p*oplach bez nebezpečí pro chráněný zájem, u něhož nebyla zjištěna příčina, např. elektromagnetické rušení, porucha systému či jiná příčina, která nesouvisí s monitorovanými fyzikálními parametry.