A GSM RENDSZER BIZTONSÁGI KÉRDÉSEINEK VIZSGÁLATA

Mérés helye: Híradástechnikai tanszék
Mobil távközlési és informatikai laboratórium
IB. 113.

A mérést készítette: Gódor Győző
2004

Bevezetés

Napjainkban a mobil távközlés rohamos fejlődésének lehetünk szemtanúi. A felhasználók egyre több mobil készüléket és ezzel együtt előfizetést vásárolnak. Így a biztonságos kommunikáció elengedhetetlen szempont. Ezért nagy hangsúlyt fektetnek az egyes rendszerek megtervezése során a biztonság, a hitelesítés és a titkosítás kialakítására.
Európában a legelterjedtebb mobil rendszer a GSM rendszer, ezért ezen mérés során a GSM rendszer bizonyos paramétereivel, és a biztonsági, illetve hitelesítési mechanizmusával ismerkedhetünk meg.

Ezen a mérésen olyan Teszt berendezéseket használunk, amelyeket mobil készülék bemérésére használnak. Egy ilyen Teszt Set egy teljes bázisállomást szimulál.

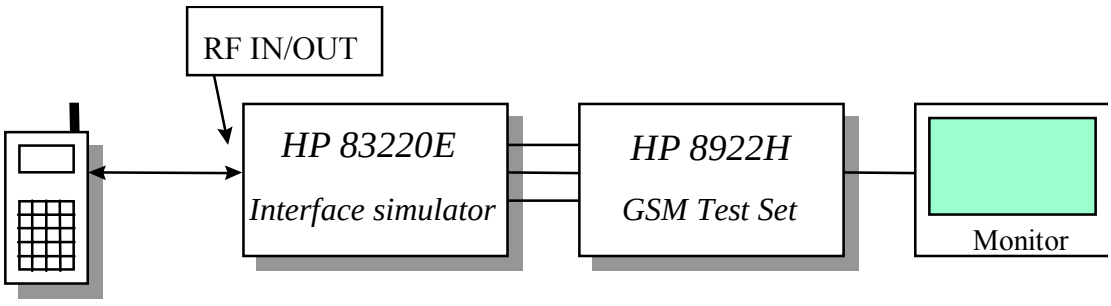
A mérés célja, hogy a hallgatókat megismertessük a Magyarországon (és máshol) használatos GSM teszt készülékek kezelésével és alapvető funkcióival

Ahhoz, hogy a mérés gyorsan elvégezhető legyen, kérjük olvassa el mindenki a *HP 8922H* kezelési útmutatójából készült rövid összefoglalót !!!

Mérési összeállítás

HP 8922H

Ezzel a készülékkel mind a 900 MHz-es, mind az 1800 MHz-es sávban lehet méréseket végrehajtani. A vizsgálandó mobil készüléket közvetlenül nem lehet a *HP 8922H* teszt készülékhez csatlakoztatni, hanem szükségünk van egy *HP 83220E* levegős interfész szimulátorra.
Mivel a teszt berendezésnek kis méretű kijelzője van, amit nem láthat minden hallgató egyszerre, ezért a display-en megjelenő információkat egy külön monitoron lehet figyelemmel kísérni.



1. ábra. A mérési összeállítás

Mérések

A *HP 8922H* berendezésen a mérés két fő részből és több alrészből áll.
Az első részben a hallgatók a méréseket lépésről lépésre, manuálisan fogják végrehajtani, míg a második részben megismerkednek a Test Set-ben rejlő bonyolultabb mérések programozott lefutásával.

Hívásfelépítés

Mivel a Teszt készülék egy bázisállomást szimulál, ezért lehetőség nyílik erről a készülékről is hívást felépíteni. Ezt azonban csak akkor lehet végrehajtani, ha a készülék "tudja" a meghívandó mobil berendezés címét, azaz az IMSI számát. Ennek a megadására több lehetőség is adódik.

- Amennyiben tudjuk a mobil IMSI számát, akkor azt az *MS Information/Signaling* képernyőn a *Paging IMSI* ablakban lehet megadni.
- Ennél egyszerűbb megoldás, ha hívást kezdeményezünk a mobil készülékről. A jelzésváltás alatt a Teszt készülék megjegyzi a hívó számát.

Teljesítmény mérés

A vivő csúcsteljesítmény az átvitt burst hasznos része alatti vivőteljesítmény átlaga. Ez a csúcsteljesítmény 2 dB-es lépésenként vezérli a bázisállomás. A 13 dBm-től 43 dBm-ig terjedő skálát 16 teljesítmény vezérlési szintre (0 szint tartozik a legnagyobb teljesítményhez), ill. öt teljesítmény osztályra osztották fel a 900 MHz-en az 1. táblázat szerint. 1800 Mhz-en csak 14 teljesítmény vezérlési szintet határoztak meg, amit 2 osztályba soroltak. Az ezen a frekvencián alkalmazott teljesítmény tartomány 4 dBm-től 30 dBm-ig terjed.

GSM 900		DCS 1800	
Teljesítmény osztály	Teljesítmény vezérlési szint	Teljesítmény osztály	Teljesítmény vezérlési szint
1	0	1	0
	1		1
2	2	2	2
3	3		3
	4		4
4	5		5
	6		6
5	7		7
	8		8
	9		9
	10		10
	11		11
	12		12
	13		13
	14		-
	15		-

1. táblázat. Teljesítmény osztályok / Teljesítmény vezérlési szintek

BER mérés

Míg analóg rendszerekben egyszerűen mérhető a vevő teljesítőképessége, addig digitális rendszerekben a beszéd-dekódoló és hibajavító eljárások miatt lehetetlen precízen meghatározni azt. Mivel még a beszéd-dekódoló előtti demodulált jelet kellene megvizsgálni, ami a zárt készülékben hozzáférhetetlen. Ennek elkerüléséhez a mobil készüléket visszacsatolt módba kapcsolják. A teszt alatt egy Pseudo Random Binary Sequence-t állít elő a teszt készülék. Ezt a downlink TCH-re modulálják helyes midambel bitekkel, korrekt keret struktúrába. A mobil ezt demodulálja és visszaküldi az uplink TCH-en. A teszt készülék ezután a fogadott, késleltetett jelet veti össze az általa elküldött jellel. A mérés során emiatt pár másodperces késleltetéssel kell számolni.
Különbözőképpen lehet bit hibavalószínűséget meghatározni. Ezek közül kettővel lesz dolgunk a mérés alatt.
A *Bit error rate* meghatározásához minden beszéd és adatbitet figyelembe vesz.
(Type I, TypeIa, Type Ib, Type II)
A *Residual bir error rate* meghatározásához csak olyan beszédkereteket használ, ami nem minősül rossz vagy sérült keretnek.
(ResType I, ResTypeIa, ResType Ib, ResType II)

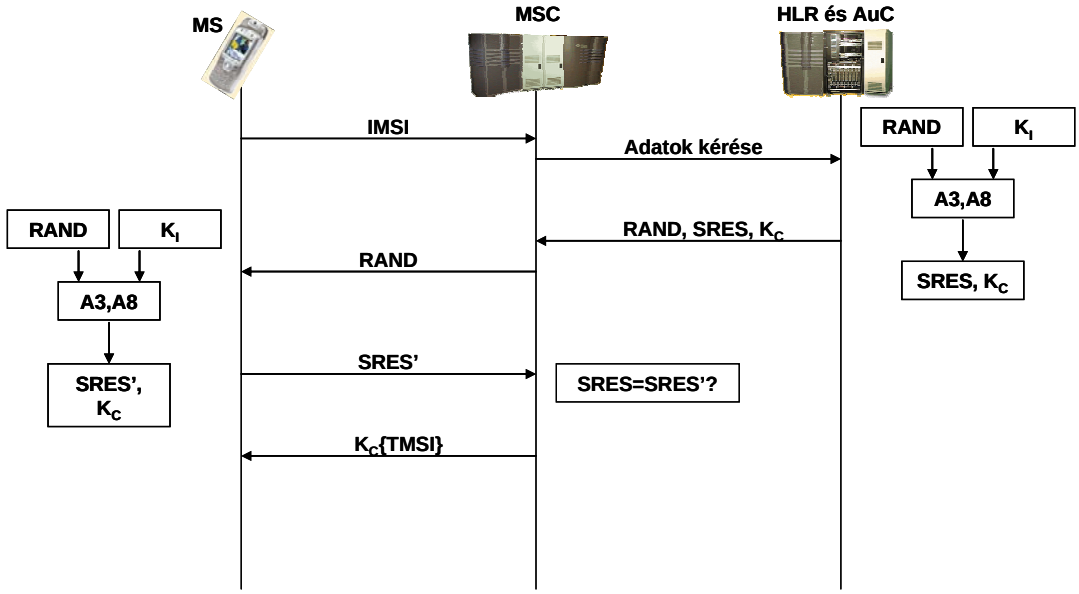
Tesztek a GSM Mobile Station Test Software-en belül

A Test software-en 16 különböző tesztet írtak meg előre.
1. MS Information
2. Hívás a bázisállomásról
3. Hívás a mobil készülékről
4. Speach Quality
5. TX In-Channel Tests
6. TX Peak Power Error
7. TX ORFS (Output RF Spectrum) due to Modulation
8. TX ORFS due to Ramping
9. RX Reference Sensitivity (TCH/FS)
10. RX Usable Input Level Range
11. RX Timebase Tuning Range
12. MS Quick Test
13. MS Flow Chart
14. TX RACH Test
15. CP End Call
16. Dualband Handover

Biztonsági és hitelesítési paraméterek mérése

A GSM rendszer biztonsági modellje az úgynevezett szimmetrikus kulcsú titkosításon alapul. A megosztott titkok a K_i és a K_c kulcsok, melyek a HLR és a felhasználó SIM kártyáján találhatók. A K_i kulcs egy 128 bites kulcs, mely egy 32 bites aláírt válasz előállítására szolgál, melyet SRES-nek hívnak, ezt az MSC használja egy kihívásra. A K_c kulcs pedig egy 64 bites kulcs, melyet a rádiós csatornánál használnak titkosításra.

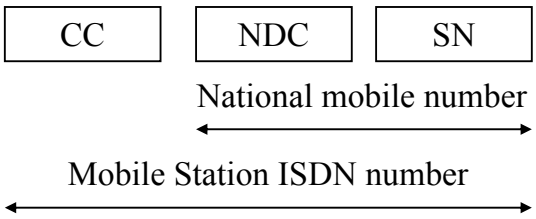
A GSM rendszer a felhasználó hitelesítését egy challenge-response (kihívás-válasz) mechanizmusa segítségével hajtja végre, melyet a 2. ábra szemléltet:



2. ábra. A GSM rendszer hitelesítése

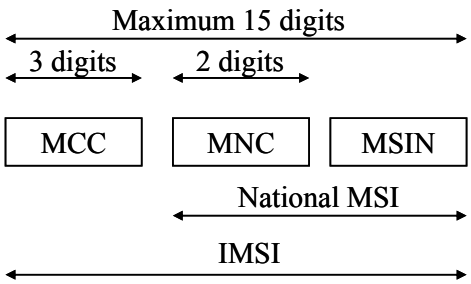
Az előfizetők anonimitása érdekében különféle azonosítókat alkalmaznak a GSM rendszerben:

- MSISDN Mobile Station ISDN Number
  MSISDN = CC + NDC + SN, max 15 digit
  - CC = Country Code, ország kód, max 3 digit 36
  - NDC = National Destination Code, nemzei cél kód, 2-3 digit 30
  - SN = Subscriber Number, előfizető száma, max 10 digit 987654



3. ábra. Az MSISDN felépítése

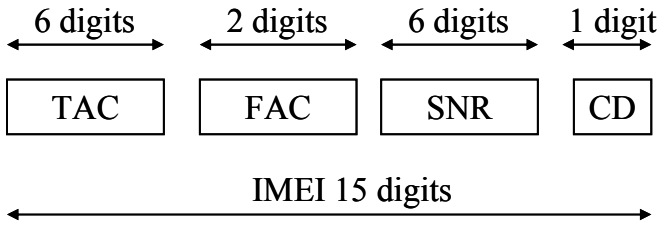
- IMSI International Mobile Subscriber Identity
  IMSI = MCC + MNC + MSIN, NMSI = MNC + MSIN
  - MCC = Mobile Country Code, mobil ország kód 216
  - MNC = Mobile Network Code, mobil hálózat kód 30
  - MSIN = Mobile Station Identification Number, mobil állomás azonosító szám 1234567890



4. ábra. Az IMSI felépítése

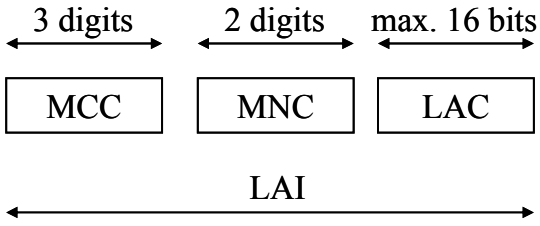
- TMSI Temporary MSI
  - Az MSC egy ideiglenes IMSI-t (TMSI) jelöl ki, ami átmenetileg az MSI helyébe lép a VLR területén.
  - Használatával a rádiócsatornák lehallgatásával nem nyerhető ki a mobil azonossága.
  - A TMSI kiosztása titkosítva történik.
  - A TMSI egy 8 jegyű hexadecimális véletlen szám.
  - Hálózati hozzáféréskor a mobil ezt a lefoglalt TMSI-t használja.
  - A következő helymeghatározáskor a TMSI változhat, ID hopping.

- IMEI International Mobile Equipment Identity
  - IMEI = TAC + FAC + SNR + (SP), CD
    - TAC = Type Approval Code, típusengedélyezési kód, központi
    - FAC = Final Assembly Code, összszerelési kód, gyártó
    - SNR = Serial Number, sorozatszám, gyártó
    - SP = Spare Digit, tartalék digit
    - CD = Check Digit, ellenőrző digit



5. ábra. Az IMEI felépítése

- LAI Location Area Identity
  - LAI = MCC + MNC + LAC
    - MCC = Mobile Country Code, mobil ország kód
    - MNC = Mobile Network Code, mobil hálózat kód
    - LAC = Location Area Code, lokációs terület kód (max 16 bit)
  - BCCH-n sugározzák, segítségével minden cella LA-hoz rendelhető.
  - Ha a mobil ennek megváltozását érzékeli akkor helyzetfrissítést (LU) kér a HLR-ben és a VLR-ben.
  - Ez azt is jelenti, hogy a mobilnak kell figyelnie a vételi körülményeket és a legjobb vételt biztosító bázisállomáshoz tartozó LA VLR-jéhez kell bejelentkeznie a BS segítségével.
  - A LAI-t a VLR adja meg amikor hívásfelépítés során a mobilt keresik. Ide mennek a paging üzenetek, amire a mobil válaszol.



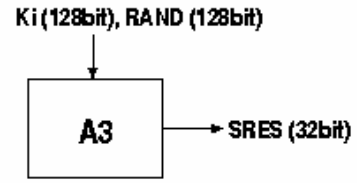
6. ábra. Az LAI felépítése

Az előfizető anonimitása érdekében egy ún. ideiglenes előfizető azonosítót is használnak (TMSI=Temporary Mobile Subscriber Indentity). A TMSI-t a hitelesítés befejeztével kapja a felhasználó. A telefon a TMSI „átvételének” megerősítésével válaszol. A TMSI abban a körzetben érvényes ahol "kiállították". A körzeten kívüli kommunikációhoz szükség van még egy ún. körzeti azonosító számra (LAI=Location Area Idendification) is a TMSI-vel együtt.

Az A3, A5 és A8 algoritmus

Az A3 algoritmus:

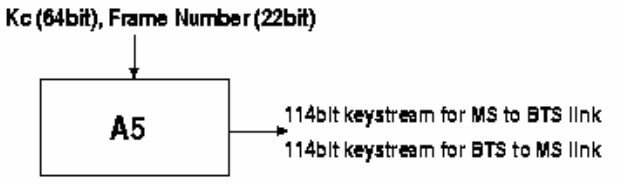
A hitelesítést szolgálja a GSM rendszerben. A SIM kártyán található K_i kulcsból, és az MSC által küldött RAND számból generál egy 32 bites kimenetet, mely az SRES válaszfüggvényt. Mind a RAND, mind a K_i kulcs 128 bites. Az A3 algoritmus működését a 7 ábra szemlélteti.



7. ábra. Az A3 algoritmus működése

Az A5 algoritmus:

A rádiós átvitel titkosítására szolgál ez a folyam-kódoló algoritmus. A folyam-kódolót minden egyes frame küldésénél inicializálni kell, melyet a session key (K_c) segítségével, és a kódolandó/visszafejtendő frame-k számával végeznek. A hívás során azonos K_c-t használnak, de egy 22 bites frame number-t választanak a hívás alatt, így generálva minden egyes frame-nek egy egyedi kulcs-folyamot.
Az A5 algoritmus Európában három különböző hosszúságú LSFR-t definiált: 19, 22 és 23 bit. A három regiszter kimenete XOR-olva van, és az XOR reprezentál egy kulcs-folyamot. Mindhárom regiszter órajellel van ellátva. Az A5 algoritmus működése a 8. ábrán látható.

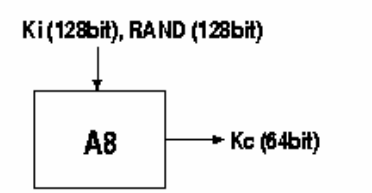


8. ábra. Az A5 algoritmus működése

Az A8 algoritmus:

Ez a GSM rendszer kulcsgeneráló algoritmusa. A K_c session key generálására használják, melyet a K_i és a RAND (két 128 bites bemenet) segítségével állít elő a

SIM kártyán a mobil készülék. A K_c kulcs egy 64 bites kulcs, melyet az A5 algoritmushoz használnak. Az A8 algoritmus működése a 9. ábrán látható.



9. ábra. Az A8 algoritmus működése

Mérési feladatok

1. Kapcsolja be a *HP 8922H* Teszt készüléket a bal alsó sarokban található gombbal, valamint a monitort. Tegye be a mérendő mobil készülékbe a Test SIM kártyát és várja meg, amíg a Test készülék felboot-ol. Kapcsolja be a mobilt és várja meg, amíg hálózatot megtalálja. Ekkor a mobil kijelzőjén vagy a *001 01* vagy *CC001NC01* jelenik meg.
2. Bekapcsolás után a *Cell Control* képernyő jelenik meg. Állítsa be a GSM900 vagy DCS 1800, aktív cellás+ felhasználási módust. Jegyezze fel a BCH csatorna számát és ennek maximális amplitúdóját, valamint a mobil készülék paramétereit.

Teljesítmény mérés

1. Kezdeményezzen hívást mind a Test készülékről, mind a mobil készülékről. Határozza meg a mobil által maximálisan ill. (működés közben) minimális kibocsátott teljesítményt. Melyik teljesítmény osztályba tartozik a vizsgált mobil készülék?
2. A hívás alatt változtassa meg a mobil készülékhez rendelt vizsgált csatornát, ill. időrést. Figyelje a kijelzőn az eredményeket. Mit kezdeményezet ezzel a megoldással? Milyen változásokat vett észre?
3. Vizsgálja meg egy GSM burst viselkedését. Kapcsoljon át a *PWR RAMP* képernyőre. Itt a *View* mezőben kiválasztva vizsgálja meg a jel emelkedését, jel esését és a felső 2 dB viselkedését. Hol, milyen mértékkel tér el a jel a szabványban foglaltaktól? A szabvány értékeket a mask bekapcsolásával lehet előhívni. Értelmezze a kapott eredményeket. Miért fontos ezeknek az értékeknek a betartása ?

Bit hibaarány mérés

1. A *Cell Control* képernyőn állítsa be a BCH számát 60-ra.
2. Váltson a *BER* képernyőre és válassza ki a *ResTypeII* -t
3. A vizsgálandó bitek számához írjon be 8200-at.
4. Állítsa a BCH amplitúdóját -102 dBm-re.
5. Ismételje meg a mérést *ResType Ib* beállítással, 250000 bitre.

Biztonsági és hitelesítési paraméterek mérése

1. Állítsa a készüléket az MS Information/Signalling állásba.
2. Jegyezze fel a készülék IMSI és IMEI számát!
3. Vizsgálja meg a hívásfelépítés folyamatát, illetve a Location Area váltásokat, ha a TMSI be van kapcsolva, illetve ha nincs!
4. Az Authentication Mode négy különféle hitelesítési mechanizmust tartalmaz (None, Full-64, Full-54 és Partial). Vizsgálja meg mi a különbség a négy megoldás között! Jegyezze fel az egyes esetekben a különféle kulcsokat, illetve a hitelesítés során kapott értékeket!
5. Vizsgálja meg, mi történik abban az esetben, ha megváltoztatja a K_i, K_c kulcsok értékeit! Tapasztalható-e különbség, ha a kulcsot hívás közben változtatjuk meg, illetve ha a kulcs megváltoztatása után kezdeményezünk hívást? Ha igen, mi lehet a magyarázat?

Ellenőrző kérdések

1. Adja meg a GSM (Primary és Extended) valamint a DCS rendszerben használt uplink és downlink frekvencia tartományokat. Mekkora az egy felhasználóra kiosztott sávszélesség?
2. Milyen GSM burst típusokat ismer? Adja meg a NORMAL burst felépítését, milyen három dimenzióban lehet felrajzolni ezt a burst-öt (rajz!!!)?
3. Miben különböznek a TypeI, TypeIa, TypeIb, TypeII bitek egymástól?
4. Mi a SIM kód? Milyen hosszú az, milyen információt tárol?
5. Röviden ismertesse, illetve rajtolja fel a GSM rendszer hitelesítési rendszerét!
6. Sorolja fel a GSM rendszerben használt azonosítókat!
7. Milyen funkciót tölt be a GSM rendszerben az IMSI? Rajzolja fel a felépítését!
8. Mire szolgál a TMSI?
9. Mire szolgál a LAI? Mutassa be a felépítését egy rajz segítségével is!
10. Röviden ismertesse az A3, A5 és A8 algoritmusokat!

Irodalomjegyzék

[1] http://www.dia.unisa.it/professori/ads/corso-security/www/CORSO-9900/a5/Netsec/netsec.html

[2] http://www.hackcanada.com/blackcrawl/cell/gsm/gsm_security.html

[3] http://www.gsmworld.com/using/algorithms/index.shtml

[4] http://jya.com/crack-a5.htm

[5] http://www.etsi.org/

[6] http://www.ietf.org/

HP 8922H GSM Test Set kezelési útmutató

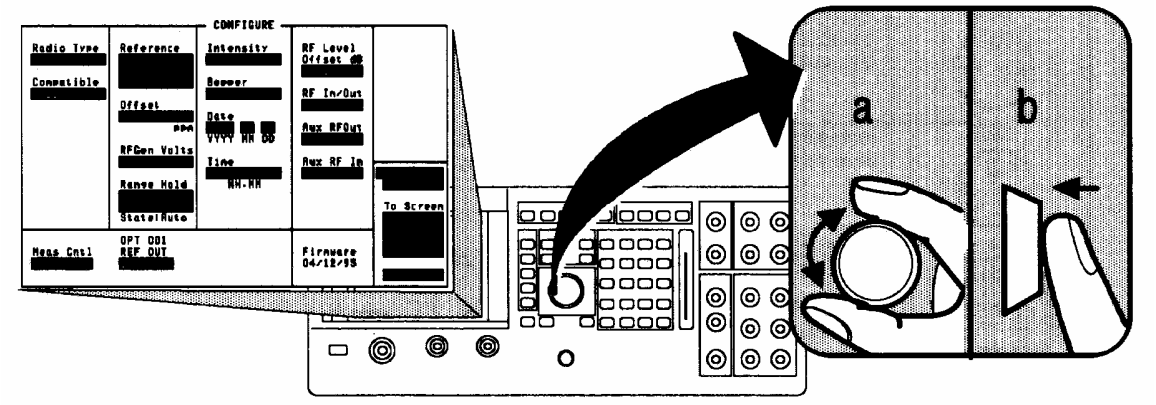
(rövid összefoglaló)

Bevezető

Ahhoz, hogy a mérés a meghatározott időkeretek között elvégezhető legyen, minden hallgatónak szüksége van az első látásra bonyolultnak tűnő Teszt készülék előzetes "megismerésére".
Mivel a mérés során nem térünk ki a készülék minden funkciójára, ezért természetesen csak az alapvető gombokat és képerőket használjuk.

Forgó gomb

A Teszt készüléken egy képernyőt, csatlakozókat és gombokat lehet látni. A gombok közül a berendezés közepén található nagyméretű forgatható, megnyomható gomb a legfontosabb. A gomb forgatásával az adott képernyőn lehet a cursor helyzetét változtatni, ezen gomb megnyomásával pedig a cursor helyén lévő mezőt lehet kiválasztani.



Mezők

Az egyes képernyőkön négy fajta adatmezőt különböztetünk meg. Ezek kívülről nem különböznek egymástól.

1. Alfanumerikus

Ebbe a mezőbe neveket, címeket lehet beírni. A forgógomb megnyomásával a képernyő jobb alsó sarkában megjelennek az ABC betűi, valamint vezérlő parancsok. Onnan egy betűt ismételten a forgógomb forgatásával ill. megnyomásával lehet kiválasztani. Ha végeztünk a karaktersorozat megadásával, akkor a mező első pozíciójában szereplő "done" parancsot kell választani.

2. Adat megadás

Ebbe a mezőbe számértéket és mértékegységet lehet megadni. Két lehetséges módon lehet ezt megtenni.

- A kijelölt mezőben a forgógomb forgatásával lehet az értéket növelni vagy csökkenteni.
- A kijelölt mezőbe a számbillentyűkkel lehet értéket beírni, amit azután vagy az *"Enter"* gombbal vagy egy mértékegységhez rendelt gombbal lehet elfogadtatni (dBm, μV). (Ezen a módon lehet mértékegységet változtatni)

3. Választás egy listából

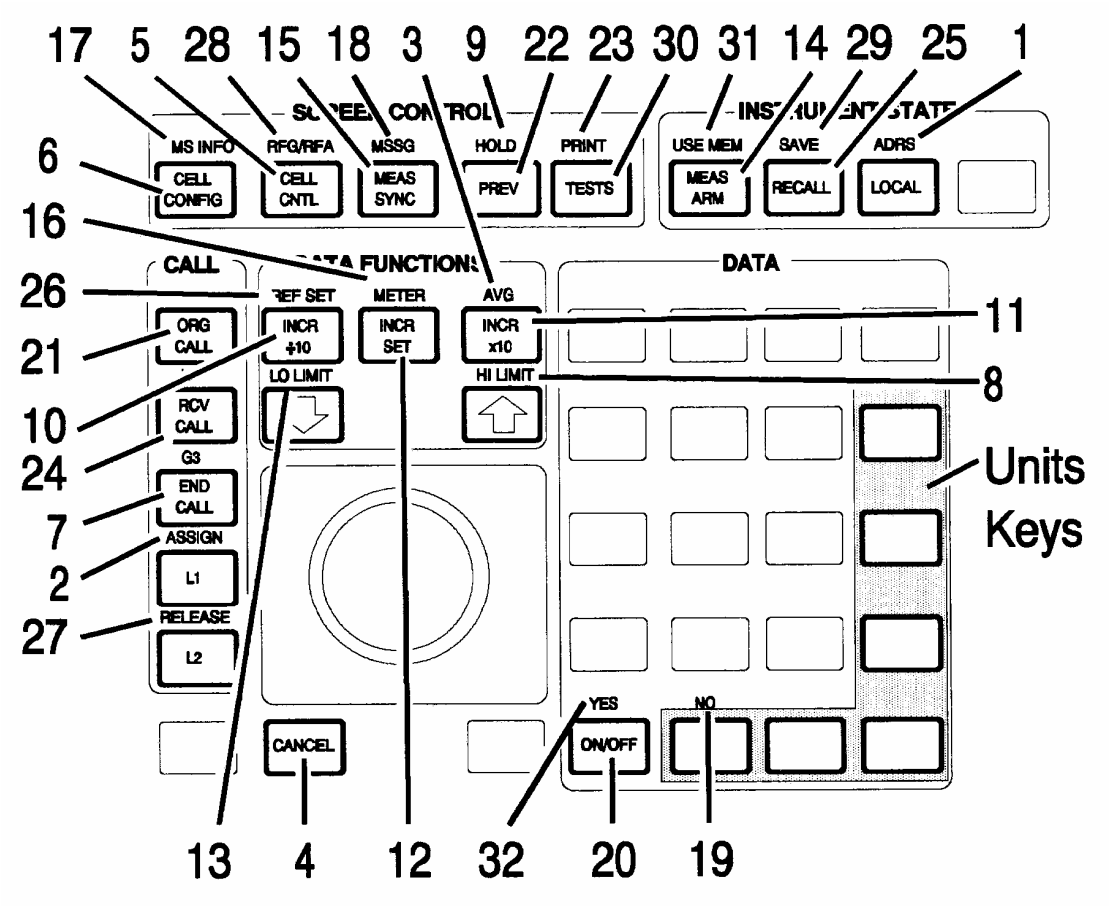
A forgógomb megnyomása után egy görgőlista jelenik meg a kijelölt mező alatt. Ebből kell egyet kiválasztani ismételten a forgógomb forgatásával ill. megnyomásával. Egy ilyen mező, ami minden képernyőn megtalálható, a másik képernyőt kiválasztó lista, ami mindig a jobb alsó sarokban található.

4. Aláhúzott megadás

Az is előfordulhat, hogy két előre meghatározott érték közül kell egyet kiválasztani, melyek egy slash-el vannak egymástól elválasztva (/). Ekkor a forgógomb elfordításával az aláhúzás jelöli az aktív értéket. Megesik az is, hogy aláhúzás helyett az aktív értéket nagybetűvel, míg az inaktívat kisbetűvel jelöli a gép.

Gombok

Ehhez a méréshez nem szükséges minden gomb ismerete. A legfontosabb gombról már tettünk említést. Mint látni lehet, a legtöbb gombhoz két-két megfeleltetést rendeltek a gyártók. A gomb fölé írt funkciót a kék *"Shift"* gombbal lehet kiválasztani. (Erre egy utalás jelenik meg a kijelző jobb felső sarkában) Ezt a gombok között a bal alsó sarokban lehet a *"Cancel"* gomb mellett megtalálni.



4. CANCEL

Egy tesztsorozatot pl. a *"Shift + Cancel"* kombinációval vagy az *"L2"*-es gombhoz rendelt abort paranccsal lehet megszakítani.

5. CELL CNTL

A gomb megnyomásával könnyen juthatunk a *Cell Control* képernyőre. A Teszt készülék bekapcsolása után is ez a képernyő jelenik először meg.

6. CELL CONFIG

A bázisállomás paramétereit lehet itt állítani.

7. END CALL

Ezzel a gombbal lehet egy hívást megszüntetni.

17. MS INFO

A gomb megnyomásával az *MS Information/Signalling* képernyőre jutunk.

19. NO

Abban az esetben , ha a teszt készülék igen/nem válasz elé állít, akkor lehet ezzel a gombbal nemmel válaszolni.

21. ORIG CALL

A gomb megnyomásával lehet a "bázisállomásról" (HP 8922H) hívást kezdeményezni.

22. PREV

A gomb megnyomásával visszatérünk az előző képernyőhöz.

24. RCV CALL

A gomb megnyomásával lehet fogadni a mobil készülékről érkező hívást. Nem szükséges a használata, ha a *Cell Control* képernyő aktív.

30. TESTS

A gomb megnyomásával a Teszt képernyőhöz jutunk. Ezzel a gombbal lehet futtatni a HP 83212B Test Software-t.

32. YES

Abban az esetben , ha a teszt készülék igen/nem válasz elé állít, akkor lehet ezzel a gombbal igennel válaszolni.

L1, L2 gombok segítségével lehet egy képernyőn két mezőhöz könnyen eljutni. Ez a képernyőn a mező melletti kis megjegyzésekből látszik. A tesztsorozat futása közben hasznos lehet.