832 :

21 for control.

811 for voice, paging, etc.

21 Control channels: Use FSK

(digital: Frequency Shift Keying,
two frequencies (?)
0, 1.)

811 ~~More~~ "voice" channels use FM.

(Analog : Frequency Modulation).

If two companies share:

each might have 21 control channels
395 "voice" channels.
416

Handset: 32 bit serial number

10 digit (?) phone number

When turned on: scans 21 control channels.

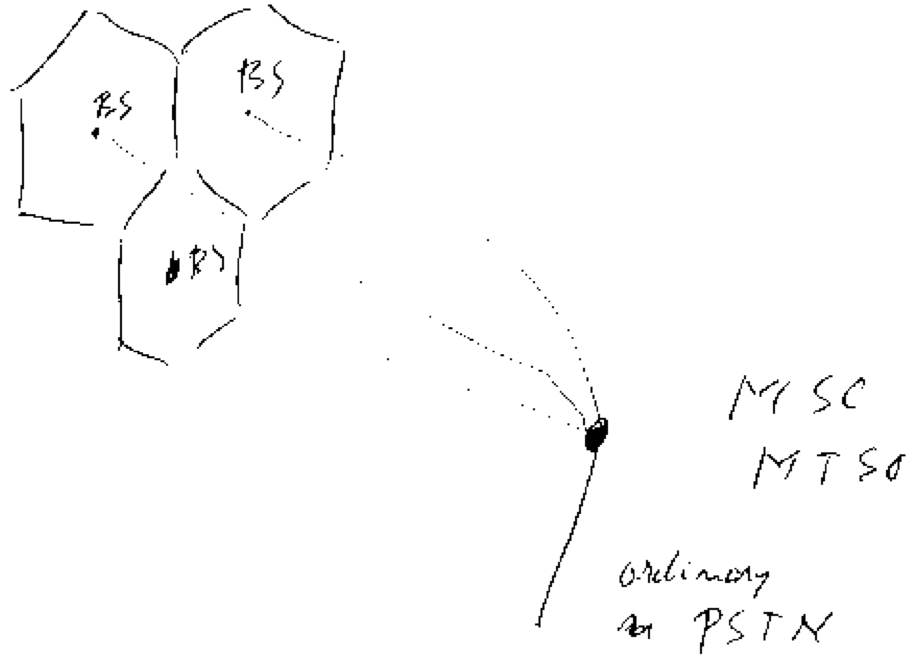
finds "strongest signal". Announces itself to Base-Station.

Explain Base-Station.

1 "Antenna" ≡ 1 Base-Station.

1 MSC ≡ several Base Stations.

Mobile Switching Center.



Each "cell", or
each "Antenna Structure" has (is) a
Base-Station. (BS)

An MSC (Mobile Switching Center) or
or MTSO (Mobile Telephone Switching
Office)
"controls" several Base Stations.

MSC or MTSO interfaces with
"ordinary" PSTN.

Abbreviations:

MTSO Mobile Telephone Switching Office

MSC Mobile Switching Center

All base-stations in a "group of cells" are connected to an MTSO.

data base, also "connection with landline network". PSTN.

There is a "Home Data base" for every user:

Reachable if you have the telephone number. (You need the phone number to reach it).

The Home data base "knows" where the customer (handset) is.

Handset turns on.

Searches for strong signal.

Reports to local MTSO or MSC.

local MTSO or MSC reports to home data base. (Possible because it knows Phone number.)

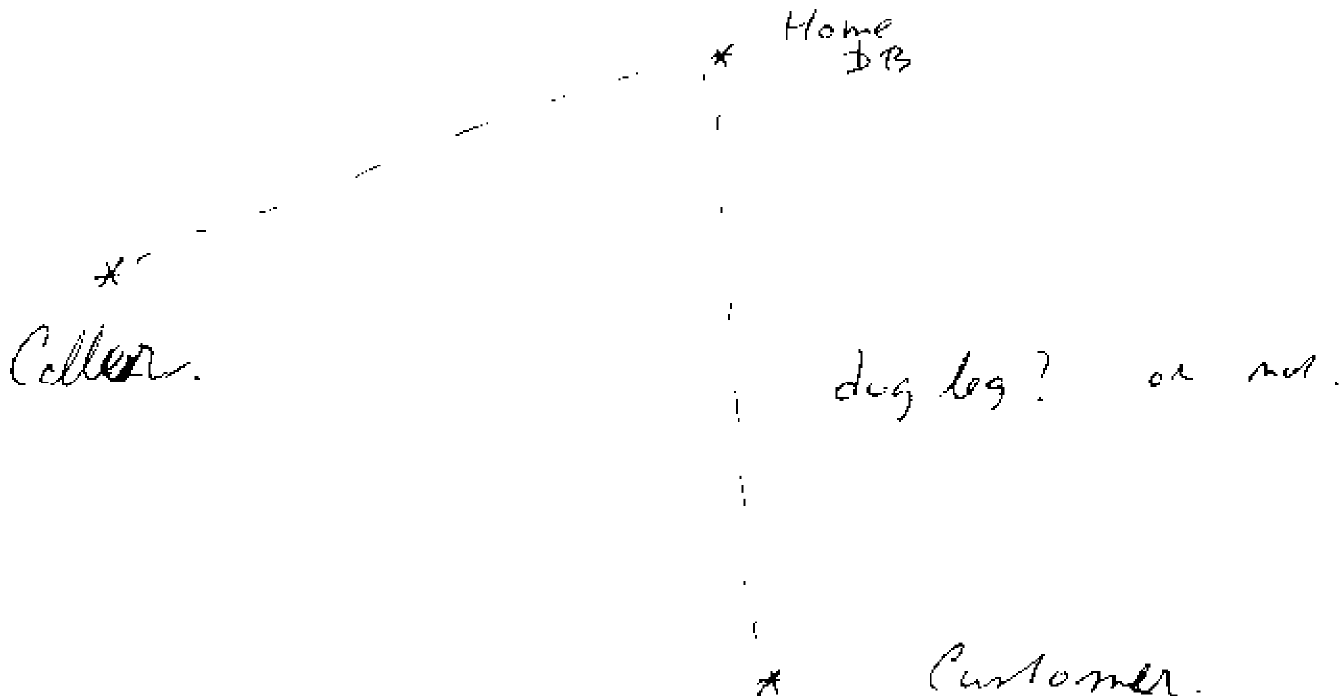
If handset is on:

Reports every ~ 15 minutes.

Incoming call:

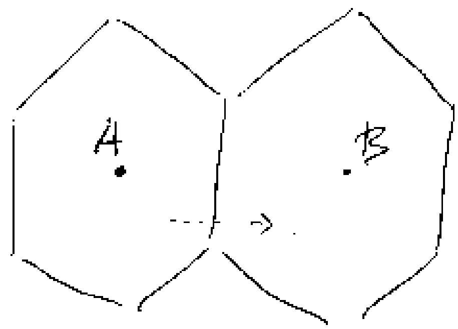
First to Home Data base.

(One way or another):



Caller "finds" customer.
(Possibly: Search in adjacent cells,).
then adjacent MSCs, etc.

HandoFF



If a customer moves from one cell to other: handoff occurs.

in A. ~~poo~~ signal strength decreases.

A asks neighbors: "who can hear this guy"?

HandoFF occurs. See Tanenbaum.

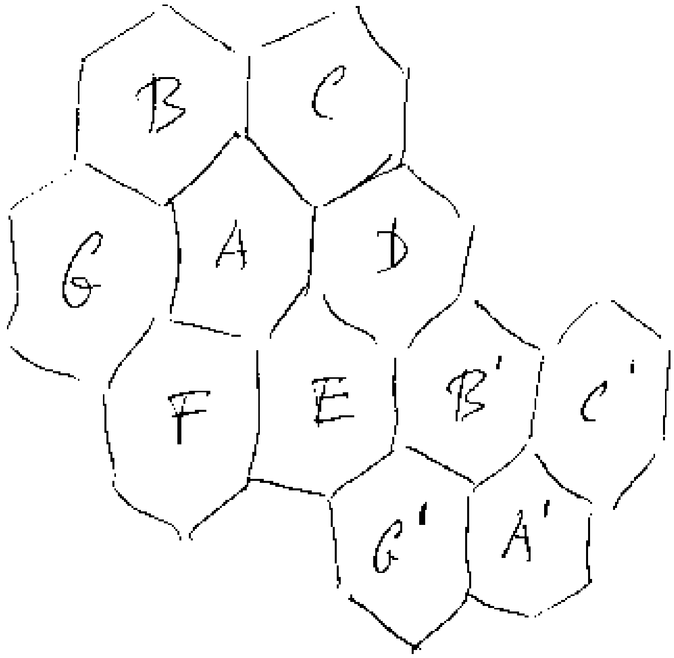
Handoff may fail!

Most important:

Frequency Re-use.

There are ~~...~~ 832 full duplex channels.

No Re-use in adjacent cells.



etc.

each cell uses ~ $\frac{832}{7} \simeq 118$ channels.
or fewer. (typically more like 40 or 50?)

Smaller cells ⟹ Lower power ⟹
Better use of spectrum
(but more handoff).

Old: 100 × 100 mile "cell" cell
1 conversation / channel.
New: 100 10 × 10 mile "cells".
~ $\frac{100}{7}$ ≈ 14 conversations/channel.

Also: lower power ⟹ lighter, cheaper handsets, longer battery life.

Battery life is major issue!

Next version of AMPS:

D-AMPS.

Digital AMPS

(Advanced Mobile Phone System).

AMPS: analog transport
digital signalling.

D-AMPS: fully digital.

Same 30 kHz simplex channels

plus more.

PLUS : TDM : 3-6 users per channel.

How is that possible?

digital voice compression. Based on Human vocal system.

down to 8 Kb/sec (kbits/sec)

or even less.

Forouzan says ~~7.5~~ 7.95 kb/s.

D-AMPS: Digital.

FDM (30 kHz channels)

plus TDM.

QPSK. (Phase Shift Keying).

Both Voice & Signalling.

D- AMPS:

In USA,

modified version in Japan.

GSM

Global System for Mobile Communication.

"The European System".

They use the name "GSM" as synonym for "cellphone"

"My GSM". Where is your GSM. etc.,

124 duplex channels.

each channel: 2 simplex links.

each link: 200 KHz wide.

8 users share a channel (TDM)

Digital: GMSK ("like" FSK).

Complicated Slot - Frame - Multiframe - ... structure.

Frequency Division separates channels (each 200 KHz wide)

Time Division allows 8 users per channel.

IS-95

Interim Standard 95.

A form of cellular phone using

CDMA

Code Division Multiple Access

and

DSSS

Direct Sequence Spread Spectrum

Technology: Qualcom.

All major manufacturers are now manufacturing "CDMA" based phones.

Which providers are using it?

(I think many).

Seems to be the best technology.

Cell phones:

First Generation: AMPS (analog transport ~10 km cells).

Second Generation:

D-AMPS (IS-136)
GSM
CDMA (IS-95)

Fully digital. cells ~10 km or smaller. (sometimes: very small).

Third Generation:
Coming Soon! (
Voice as good as PSTN now
Datarate ~ 144 kb/s.
Interface to Internet

PCS: "Personal Communications".
Any Second Generation Technology.
Including Short Message Service.

Final: Friday 12/12/2003.
Make sure to ask questions:
now, or 12/05, or 12/09, not after 12/09.

Network Security (Message Security).
Tanenbaum Ch 8

What do we expect from a <u>security-tool</u>?

- Confidentiality. (Privacy)
  (Others can not read your mail).

- Authentication.
  (You want to be <u>sure</u> of the senders identity.
  No "spoofing").

- Integrity.
  (You want to be <u>sure</u> the message has not been modified on the way).

- Non-Repudiation.
  ~~(You want to be able to <u>prove</u> you got the message, what time, etc.)~~
  Example:
  (You want to be able to <u>prove</u> the other guy got your message).

Related issue: Time stamping.
You want to be able to <u>prove</u> at what time you sent / received a message, ~~and~~ incl. content.

Related area:
"Zero knowledge proofs".

There is more to ~~sec~~ computer security than network security.

E.g. Access to Resources.

Permission to log on
(Password).

Permission to read certain files.
(~~Only~~ (e.g. personel files, salaries).

How do you make a computer secure?
(Lock it in vault, without remote access).

~~Back to~~
Who has heard of one-time passwords?

Is (Network) Security the same as Secrecy ?

No :

(1) Look at the 4 points.

(2) Traffic Analysis!

I may be able to monitor your encrypted traffic.

Can not decrypt it. But:

Draw conclusions from volume, possibly who you are talking with, etc.

Example: "third U.S. Army" in England, 1944.

Al Queda now?

How do we achieve network security ?

Let's start simple:

How do we achieve Privacy ?

Cryptography

(1) Mono-Alphabetic Substitution.

Simple!

I B M (Ceasar Code).
H A L (Arthur C. Clarke, Odysee 2001)

(2) Block-Substitution.

(Let's be binary)

Block of k bits replaced by other block of k bits. 1-1.

2^k different blocks of k bits.

$(2^k)!$ different maps.

too many possibilities.

We need a key so that given the key both the forward map (encryption) and the backward map (decryption) can be found.

1 key: "Symmetric-Key" Encryption.

"History Dependent" encryption schemes:

Message (Cleartext) $B_1, B_2, B_3, \ldots, B_{k-1}, B_k, B_{k+1}, \ldots$ (Blocks)

Encrypted (Cyphertext) $\hat{B}_1, \hat{B}_2, \ldots$

$\hat{B}_k$ depends on

B_k <u>and</u> $\underbrace{B_{k-1}, B_{k-2}, \ldots, B_1}_{\text{History}}$

Still: we need a <u>key</u>.

Symmetric-Key cryptography.

Kerckhoff's principle:

The <u>algorithm</u> is public.

The <u>key</u> is secret.

For <u>implementability</u>,

<u>usability</u>.

Example of "Block Substitution" with characters.

Say we we have 128 characters. (ASCII).

No, let's do it first with three characters.

text: ~~Hi there~~ ~~You are~~ ~~1 3 2 2 4 8 t~~ 1 3 1, 2 3 1, 2 3 2

say $c_1 \; c_2 \; c_3 \; c_4 \; c_5 \; c_6 \; c_7 \; c_8 \; c_9$

Blocks: $B_1 = (c_1, c_2 \; c_3)$ $B_1^T = \begin{pmatrix} c_1 \\ c_2 \\ c_3 \end{pmatrix}$.

$B_2 = (c_4, c_5, c_6)$

$B_3 = (c_7, c_8, c_9)$

Find a 3×3 matrix

$$S = \begin{pmatrix} s_{1,1} & s_{1,2} & s_{1,3} \\ s_{2,1} & s_{2,2} & s_{2,3} \\ s_{3,1} & s_{3,2} & s_{3,3} \end{pmatrix}$$

$\hat{B}_i^T = S \, B_i^T \mod 3$.

(~~te~~ $\hat{b}_{i,j} = \sum_{k=1}^{3} c_{j,k} \, b_{i,k} \mod 3$).

Better choose S such that it is <u>nonsingular</u> in $\mathbb{Z}_3$.

$\exists\ S^{-1}$, $S.S^{-1} = S^{-1}.S = I$

$$\sum_{j=1}^{3} s_{ij}\, s^{-1}_{jk} \bmod 3 = \delta_{ik} = \begin{cases} 1 & i=k \\ 0 & i \neq k \end{cases}$$

$\hat{B}_i^T = S\,B_i^T$

$S^{-1}\hat{B}_i^T = S^{-1}S\,B_i^T = B_i^T$

Now with ~~128~~ 131 characters ~~(A~~ (say ASCII) (!)

S is a ~~128 * 128~~ 131 * 131 matrix,

with an inverse S^{-1} ~~(in $\mathbb{Z}_3$)~~

(Why 131 and not 128? 131 is prime! $\mathbb{Z}_{131}$ is a field)

S, S^{-1} must be 131 * 131 matrices, with

$$\sum_{k=1}^{131} s_{i,k} \cdot s^{-1}_{k,j} = \delta_{ij} \qquad s^{-1}_{k,j} = (S^{-1})_{kj} \text{ not } (s_{kj})^{-1}.$$

This was the <u>Hill</u> Cypher.

The size (of the blocks) must be equal to or larger than the number of characters.

A Hill-Cypher of <u>large</u> size is pretty good, <u>but</u>:

~~But~~ H

Breakable with "known plaintext" attack.

Also: hard to transmit, store the key! ($m \times m$ ~~[illegible]~~ $= m^2$ numbers)

Another Block Cypher:

Size m.

Now digital.

Message = $(b_1\ b_2\ b_3\ \cdots)$ (bits).

Blocks $B_1 = (b_1, \cdots b_m)$

$B_2 = (b_{m+1}, \cdots b_{2m})$ $b_{i,j} = b_{(i-1)*m+j}$

etc.

Key = $(k_1, \cdots, k_m)$ (bits)

$$\hat{b}_{i,j} = b_{i,j} + k_j \mod 2$$

$$= b_{i,j} \oplus k_j \quad \text{exclusive or}$$

$$b_{i,j} = \hat{b}_{i,j} + k_j \mod 2.$$

Very easy to break with "Known plaintext" attack:

If for at least one block B the enemy knows B and $\hat{B}$:

$$k_j = b_j + \hat{b}_j \mod 2.$$

The Hill cypher: (size n)

If for well-chosen $B_1, B_2, \ldots, B_n$
(each block of size n)

you know $\hat{B}_1, \ldots, \hat{B}_n$,

you can <u>compute</u> S and S^{-1}.

"Known Plaintext" Attack.

Tanenbaum pp 738 - on.

DES Data Encryption Standard.

Block Cypher.

Blocks of 64 bits.

(~~Cyp~~ Plaintext and Cyphertext).

Originally 56 bit key.

Was found too short.

<u>Complicated!</u>

Now: "Triple DES":

Block Cypher

Blocks of 64 bits

112 bit key.

(really: two 56 bit keys).

Symmetric Block Cypher

Implemented in hardware (Silicon).

K : key.

T_K : Transformation

$$\hat{B}_i = T_k B_i$$

$$B_i = T_k^{-1} \hat{B}_i$$

if you have k (key), it is "easy" to find T_k, T_k^{-1}.

Chaining (to give the system memory)

$$\hat{B}_i = T_k \left(\hat{B}_{i-1} \oplus B_i \right) \quad \text{(encryption).}$$

Encryption: have B_i ~~(new block)~~ (new plaintext block)

$\hat{B}_{i-1}$ (previous cyphertext block)

first: compute $\hat{B}_{i-1} \oplus B_i$ (bitwise exclusive or)

then compute $\hat{B}_i = T_k(\hat{B}_{i-1} \oplus B_i)$.

Decryption:

<u>know</u> $\hat{B}_i$, $\hat{B}_{i-1}$

Compute $T_k^{-1} \hat{B}_i = T_k^{-1} T_k (\hat{B}_{i-1} \oplus B_i)$

$$= \hat{B}_{i-1} \oplus B_i$$

$$B_i = \hat{B}_{i-1} \oplus T_k^{-1} \hat{B}_i$$

Alternative form of chaining:

$$\hat{B}_i = T_k (B_{i-1} \oplus B_i)$$

Chaining: No longer mono-alphabetic substitution.

AES

Advanced Encryption Standard.

(Will replace DES ?)

Tanenbaum pp 741 - on.

Not in CIS 451.

Symmetric - Key encryption schemes:
(in particular DES)

Good for privacy.

Relatively easy to implement.
Fast (one chip can do ~ 30 Mb/sec ?).
(quoting from memory). (?)

Problem. Key management.

~~Not so good for~~

- Privacy: OK.
- Authentication: OK. ("Redundancy in text"). (but: man in the middle, reflection)
- Integrity: OK. (but).
- Non-Repudiation: Not OK! (Shared key).