



Newsletter #5

Table of Contents

Editorial
by MsMittensp. 3

Random Numbers Randomized (C++ Implementation)
by shantz.....p. 4

Legacy Devices
by ouroborosp. 7

The New World Order: Terror and its Impact on Society
by Negativep. 9

Intrusion Detection
by 3ntropy.....p. 12

Number Conversion
by MrLeachy.....p. 16

MsMittens' Editorial

In the last couple of months we have seen some activity in regards to terrorism and to cyber-terrorism. And it is of no surprise that for much of the world we have become worn of the talk of war. It is in our face everyday, whether it is a physical war, a war of words or a cyberwar, it has become very prevalent within our overall society.

We re-mourned the loss of those in the September 11th attacks on the World Trade Centers. For many, it was an attack that we could not fathom. But I did read an interesting article in the *Skeptical Inquirer*, a publication who's sole goal is to challenge the things we think we believe and challenge specifically those things we believe without evidence or scientific enquiry. The article, entitled *A Skeptical Look at September 11th: How We Can Defeat Terrorism by Reacting to It More Rationally*, compares the effect of September 11th to other types of "disasters".

It is interesting that it pointed out that the 2,800 deaths (approximate – I don't think that a true final figure will be released fully for a while) pales in comparison to other tragedies such as the Indian Earthquake in early 2001. Approximately 20,000 people died. We did not see the World mourn that tragedy to the same extent as we did September 11th. We might suggest that it was because this was a natural disaster and nothing could have been done but given that most of the hardest hit areas were areas of great poverty. Simple but strong housing could have made a difference.

And what of terror at home? Approximately 15,000 people each year are killed by homicide. Every 15 seconds, a woman is being beaten by a partner (<http://www.safepass.org/two.html>). What about their terror? Evidently, it's not as important enough for us to call 9-1-1 to save someone's life. Only if CNN shows it 24/7 does it become our problem.

This past month we saw the serial killer Sniper on the rampage killing at random, creating a new terror for people in Maryland to deal with. I would not be surprised, once all is said and done, if these attacks were continuations of the terror attacks by Al-Quaeda. It would seem that there is a belief that it is necessary to cause terrorism and fear in this day and age. I've recently been watching Adam-12, a Cops show from the mid-late 1960s, early 1970s, and have been reminded as to how simpler and how safer life seemed back then. Maybe we were more sheltered.

The last bit of terrorism that is definitely on the rise is cyber-terrorism. And the biggest question has always been: would the Internet survive such attacks? I think the answer is yes based on recent activity. Attacks on the 13 DNS Root servers showed the Internet more than capable. An hour DoS against these servers didn't affect many people. This would be largely due to the size of the Internet today. Had this attack been done in the late 80s or early 90s I think the results would have been different.

But recently there have been increases in the number of port 137 scans. Incidents.org is showing high response to these scans. I suspect that many of these are from Bugbear and Scrup worms/viruses and perhaps some other activity that has yet to be defined. If it is simply scans and Bugbear/Scrup then it is a livable and easy solution to these problems: firewalls and anti-virus software. If it's not, then we might truly see something that could really after us. And maybe put us in fear of venturing on the Internet.

Our true key to fighting any terrorism – whether cyber or physical – is knowledge. And that is what this, albeit a bit small, issue is about: gaining knowledge about the events around us. I hope you enjoy and if you want to submit articles, replies to the editor, raves, rants, whathaveyou, drop me a line at AntiOnline or send me an email at msmittens@msmittens.com

Random Numbers Randomized (C++ Implementation)

by Shantz

Sometime or the other you need to generate random numbers for your programs as they play a very important role in computer applications, especially in simulations. A particularly useful random number sequence is the "uniform random number sequence". It has a specified set of numbers from which the sequence draws its random numbers. In each position of the random number sequence, any no. from the set is equally likely to occur.

Because a random number sequence is supposed to be random, there can't be any computer algorithm that iteratively computes truly random numbers. The instructions that constitute an algorithm are deterministic rules-knowing them tells you the next number. However, some functions do produce sequences of numbers that appear to be random. These sequences are called "Pseudorandom number sequences", although most people are imprecise and drop the prefix pseudo.

The C++ stdlib library provides 2 functions that are useful in generating pseudorandom number sequences. They are rand() and srand() and they are declared in stdlib.h. Function rand() takes no parameters. Each time it is invoked, it returns a uniform pseudorandom number from the inclusive interval 0 to RAND_MAX, where RAND_MAX is an implementation dependent preprocessor macro constant defined in stdlib.h. In most implementations, the generation of the current pseudorandom number is a function of the previously generated pseudorandom number. The generation of the first pseudorandom number by a program is based on a similar function of an initial value, called the seed, that is supplied to the pseudorandom number generator.

The program given below generates 5 pseudorandom numbers.

-----Code Begin-----

```
#include <iostream.h>
#include <stdlib.h>
int main()
{
for(int i=1;i<=5; ++i)
{
cout<<rand()<<endl;
}
return 0;
}
```

-----Code End-----

But when you run this program, you will see that every time the program is run, the same set of 5 numbers is generated. Why is this??. Well, this repetition is part

of the design of the function so that while the program is being tested or examined, it is possible to reproduce the same statement execution sequence.

However, if you want to produce a different sequence of pseudorandom numbers, the function `srand()` is used. Function `srand()` expects an unsigned int as its parameter which is used to set the seed for generating the first pseudorandom number. Once the seed is set, `rand()`, should produce a different sequence of random numbers. In the program given below, the user provides the seed value that is to be passed to `srand()`.

————Code Begin————

```
#include <iostream.h>
#include <stdlib.h>
int main()
{
cout<<"Random number seed (number): ";
unsigned int seed;
cin>>seed;
srand(seed);
for(int i=1;i<=5; ++i)
{
cout<<rand()<<endl;
}
return 0;
}
```

————Code End————

Now, here if the user has to undergo the hassles of providing the seed every time and if we write a constant no. as the seed in the source code itself, it will again generate the same sequence every time. So, we use the current time as the basis for the seed value because that way, the seed should be different for each run of the program. The current time is determined using the function `time()`, which is defined in the time standard library. Function `time()` returns a value of type `time_t`, which is an integral type and has to be type cast into unsigned int before it can be passed to `srand()`. An implementation for such a program is given below.

————Code Begin————

```
#include <iostream.h>
#include <stdlib.h>
#include <time.h>
int main()
{
srand((unsigned int) time(0));
for(int i=1;i<=5; ++i)
{
cout<<rand()<<endl;
}
return 0;
}
```

```
}  
-----Code End-----
```

Now, you will see that every time the program is run, a new sequence is generated. But many times, we need to generate integral numbers between two integral values. Like I recently made a Cricket match simulator and I needed to generate a number between 1 and 6 for the runs.

For such situations, we develop a function that allows us to pass the lower value and higher value between which the random number is to be generated (inclusively, i.e., including both the higher value as well as the lower value)

```
-----Code Begin-----  
int Random(int Low, int High)  
{  
int IntervalSize=High-Low+1;  
int RandomOffset=rand()%IntervalSize;  
return Low+RandomOffset;  
}  
-----Code End-----
```

Now, you can use this fuction in any of your programs and call it whenever needed it. But, remember to call `srand((unsigned int) time(0))`; before calling this function. Also, you may want to palce a simple check in the above function to check whether Low is less than High or not.

So, that's it for now. Hope I have been able to make you understand properly this simple but sometimes overlooked concept.

Let me know if i missed something or if i was wrong somewhere.

Creative type of person? We're looking for cryptographic puzzles, challenges and other security type fun. Crosswords, word finds, etc with a security bent are welcomed. Make sure you have AO Newsletter in the subject line. Submit to msmittens@msmittens.com by Friday January 10, 2003.

Legacy devices?

by ouroboros

"Dell retained legacy ports, such as serial, parallel, and PS/2, but also included cutting-edge connections such as FireWire and S-Video out..." — Computer Shopper, Sept 2002, by Stephanie Bruzzese, Jon L. Jacobi, Dan Littman and Brian Nadel

God Dammit! Am I that old?

I remember the days of the Apple 2e like it were yesterday...well perhaps not 'yesterday', since a lot of the time in between is lost in a haze of adolescence. I do remember, however, my first computer (the one that only I could figure out, while my parents just nodded vacantly when I described the 'Home' and 'Back' buttons on the Netscape browser that the college that I attended gave to me for free for signing on to the university network for 10 dollars per (enrollment) year. (Netscape 1.1, I think).

And here comes the advent of USB, FireWire (all 3 identical protocols apply...IEEE, FireWire, i.LINK), 802.11b and recently 802.11a, not to mention the public access to ADSL and cable connections (back in the day, a T1 connection rendered one a god amongst users.) Now, though, if one has less than a 56K modem, one is laughed at...the connection speed still labels a person, (a lesson in itself, methinks).

Connection to what?

...everyone else.

Long gone are the days of the BBS and the (then) Remote Server, where access to the FTP was full access, and nobody worried; and the admin knew and remembered all of the users on his/her "network".

But I digress...

I have recently come to the realization that I am getting old in this world, for the time of the 'cyber'naut is here...a totally connected world where all beings are qualified and quantified, but at the same time,,,disconnected.

The thought that intrigues me the most is that my daughter, who is 6 weeks old today, will never know a world without a computer, and the binary connections that it offers. My parents, her GRANDPARENTS, have and know how to USE a computer. It may not sound too spectacular to some, but to a person that grew up without a computer as a daily fixture will understand.

But, back to the point...how long before all computers will be instruments of our

own design, meaning a mainboard and a processor in a little 5x4 case, with a dozen USB and/or FireWire ports exposed, intent on having a HDD or two, a Video Card, Ethernet card, Sound card, RAM rack, etc connected to it? Vaguely reminds me of the Borg, from Star Trek...plug in what you need and it shall be yours.

The possibilities are limitless and very welcome, and I enjoy the challenge of keeping up with all of them...but it is very exhausting...although I fear that the new generation(s) of users will neglect the basic aspect of using a computer, which is...KNOWING HOW IT WORKS...

Just plugging into a PnP system and expecting it to work is dismissive and insulting to those who have experimented and gained knowledge through 'toying' with the hardware involved. I'm certain that I could poll 100 kids that are under the age of 20, and 99% of them couldn't tell me that the colored(red, usually) should be connected to Pin 1. (or tell me what the difference is. :))

Go Technology! and Go User Ability!, but don't forget us, the people that fix your problems and remind you to make sure that the power strip hasn't tripped, and can double your RAM in 30 seconds flat (instead of paying BB \$30 to do it for you), and can, without even trying, memorize the commands for mounting and unmounting drives, defaulting to a DOS prompt, clearing the event logs of any OS, or just accessing the BIOS in your particular computer.

"Can I get on the "internet"?" Yeah, you can.....maybe with your Legacy device....

Ouroboros

We are looking for stories for our next issue. If you want to share more material about C, C++, PHP, Intrusion Detection, Honeypots or Honeynets, submit an article by the date below. Make sure you have AO Newsletter in the subject line. Submit to msmittens@msmittens.com by Friday January 10, 2003.

The New World-Order: Terror and its Impact on Society

by Negative

The three terror-waves of our times.

Terror-waves are not new. Everytime when our society evolves fast and becomes complex, and civil groups have the feeling they are being marginalized, a terror-wave comes up. We had one at the end of the 19th century when anarchists terrorized Europe (the cause: the industrialization), we had one in the 1930's when extreme-right terrorized the world, and now we have Al-Qaeda.

Just like the anarchists in the 19th century, Al-Qaeda won't stop until the cause goes away. They will continue to attack the symbols of the arrogance of power. And those symbols happen to be American.

Al-Qaeda after Sept. 11.

It's been relatively quiet for about a year after September 11, 2001. That year is what Al-Qaeda needed to integrate in local terrorist groups. There's no coherence between their actions anymore. The fact that the recent attacks (attacks in Tunisia and Pakistan, attacks on American soldiers in Kuwait, attack on the French-Belgian oil tanker 'De Limburg') fall together gives the impression that they are being centrally organized. That's not the case though. The recent uprising has everything to do with the local situation in Kuwait and Bali. Those attacks didn't require technological means. They didn't require planning. Al-Qaeda is not able anymore to do something like the WTC-attack.

That doesn't mean Al-Qaeda ain't dangerous anymore. The recent terrorism is harder to fight than the one from before Sept. 11, just because of the fact that it isn't centralized anymore.

Terror and Islam.

It is tempting to blame the Islam for what's been happening. It also is wrong. The recent anti-terrorism campaign are pretty effective. More effective than the ones in the past. It's easy - and dangerous! - to think that we're on the eve of WW III. Panick is a bad advisor: if you panick, you'll start looking for an enemy, and you'll use violence on that enemy.

That's what's happening now, and that's only going to make things worse. Thinking about nothing but military counter-measures will make things worse, because it gives the impression that an arrogant Western 'union' thinks about nothing but their own safety, and doesn't care about the rest of the world. It is dangerous to not think about the real cause of the terrorism. It is dangerous to

blame Islam, because Islam has nothing to do with the real cause.

Bin Laden though does everything to make us believe it IS related to Islam. Bin Laden's ambitions are the ones of every messiah: he wants to become the khalif of the Muslim-world. That's why he tries to involve Islam. That's not as dumb as it sounds: every religion once started as a sect that got lucky. Bin Laden uses the humiliation of the Middle-East, with the Palestinian cause as his best weapon. That explains why he's so popular in the Muslim-community... to them, Bin Laden is a modern Robin Hood.

Comparison with the 'older' terror-waves.

The terror-wave of the 1900's is the only terror-wave that was reacted upon correctly. Don't be mistaken: that terror-wave was a lot worse than what's happening now: presidents were murdered, government-buildings were bombed,... The reaction? The bourgeois-state was reformed in a state where workers got a chance, thereby taking away the source of the anarchism.

The 1930's terror-wave (fascism) was reacted upon wrong, and finally led to WW II.

The conclusion is simple: do we really want WW III? Do we really want a replay of what happened in the 1930's? We're going in that direction...

The current situation is perfectly comparable with the one at the end of the 1900's: a globalizing world, an industrial revolution, a rift between the rich and the poor. That rift is only growing, and our nonchalance towards that rift is frigtning. We should have learned a lesson from that first terror-wave. But no, Mr. Bush doesn't like to learn.

The US.

American neo-conservatives see the recent terror-waves as a gift. A gift that will finally allow them to establish the foreign policy they've been wanting to establish since the 90's.

They see America as the only light in this dark world. They are convinced that America should use its military supremacy to offer the world stability. They use 11/9 as an alibi to vote new laws. New laws that are nothing less than freedom-threatening.

The neo-conservatives don't care about the terrorism: Clinton made a plan to capture Bin Laden from Tadzjikistan. The neo-conservatives made sure that plan didn't work out. Bin Laden fitted perfectly in their plans. And so does Saddam. The - unavoidable - upcoming war in Iraq will be a test. A test to prove that the States have entered a new era.

The real problem?

Nuclear weapons are NOT the problem: Iraq needs at least two more years to manufacture a nuclear weapon IF they can get their hands on enriched uranium (they never succeeded to get that stuff in the past).

CIA-officials have confirmed last week that it is highly unlikely that Saddam will ever use nuclear weapons. Using them would be suicide, and he knows that. The only case where he will use mass-destruction weapons is when he feels trapped. And that's just what might happen.

The States keep pushing on the fact that it is all about nukes. A leaked Pentagon-document showed a couple of weeks ago that the States themselves are willing to use nuclear weapons THEMSELVES against China, Syria, Russia, Iran, Iraq and North-Korea.

If it really was about nuclear weapons, the States should go after North-Korea. That country DOES have nuclear weapons.

It's all about nukes? Yeah right...

Europe.

Where does this all leave Europe? Europe is the only power able to stand up against America, IF the Europeans unite. And that's not happening right now: Spain (with Aznar), Italy (Berlusconi), The Netherlands (Balkenende) are on America's side. Is it really a coincidence that those countries are right-wing? Still, Europe is the only alternative for the new American world order.

Newsweek made a prediction a while ago: within ten years, America will lose its world-power to Europe, possibly with Blair as its leader.

That's not as crazy as it sounds: the States are not as powerfull anymore as they used to be after WW II: Europe is more important when it comes to the world-economy than the States. It's unimaginable that the greatest economical world-power (Europe, that is) plays the second fiddle when it comes to politics. The only conditions for that Newsweek-prediction are ambition (a united, ambitious Europe), and a continuing American recession.

Creative type of person? We're looking for cryptographic puzzles, challenges and other security type fun. Crosswords, word finds, etc with a security bent are welcomed. Make sure you have AO Newsletter in the subject line.

Submit to msmittens@msmittens.com by

Friday January 10, 2003.

Intrusion Detection

by 3ntropy

The best way to leap into the subject of intrusion detection and hit the ground running is to consider one of the most famous intrusion cases that has ever occurred, when Kevin Mitnick successfully attacked Tsutomu Shimomura's system. This attack enables us to consider two techniques still quite effective today, and we can identify many of the important issues related to intrusion detection for future discussion.

Our source for this information is drawn from Shimomura's post on the subject. If you want more information on the subject, or to get expanded versions of the quotations you see here, refer to tsutomu@ariel.sdsc.edu (Tsutomu Shimomura), comp.security.misc (date: 25 Jan 1995).

Exploiting TCP

The techniques Mr. Mitnick used were technical in nature and exploited weaknesses in TCP that were well known in academic circles, but not considered in system developers. The attack used two techniques: SYN flooding and TCP hijacking. The SYN flood kept one system from being able to transmit. While it was in a mute state, the attacker assumed its apparent identity, and hijacked the TCP connection. (For further information regarding Session Hijacking refer to [3ntropy.Session.Hijacking&Spoofing.txt](#)) Mitnick detected a trust connection between two computers and exploited that relationship. Nothing has changed since 1994; computer systems are still set up to be over trusting, often as a convenience to the system administrators.

SYN Flooding

When an attacker sets up a SYN flood, he has no intention to complete the three-way handshake and establish the connection. Rather, the goal is to exceed the limits set for the number of connections waiting to be established for a given service. This can cause the system under attack to be unable to establish any additional connections for that service until the number of waiting connections drops below the threshold. Until the threshold limit is met, each SYN packet generates a SYN/ACK that stays in the queue (which is generally between 5 and 10 total connections), waiting to be established.

Each connection has a timer; a limit to how long the system waits for the connection establishment. This timer is usually set for about a minute. After the time limit has been exceeded, the memory that holds the state for that connection is released and the service queue count is decremented by one. After the limit has been reached, the service queue can be kept full, preventing the system from establishing new connections on that port with about 10 new SYN packets per minute.

Covering His Tracks

Because the only purpose of the technique is to write, it doesn't make sense to use the attacker's actual Internet address. The attacker is not establishing a connection; he is flooding a queue, so there is no point in having the SYN/ACKs return to the attacker. The attacker doesn't want to make it easy for folks to track the connection back to him. Therefore, the source address of the packet is generally spoofed. The following IP header is from actual attack code for a SYN flood. At the very bottom, notice the daddr and saddr for destination and source address, respectively.

```
/*Fill in all the IP header information */
packet.ip.version=4;          /* 4-bit Version */
packet.ip.ihl=5;              /* 4-bit Header Length */
packet.ip.tos=0;              /* 8-bit Type of Service */
packet.ip.tot_len=htons(40); /* 16-bit Total Length */
packet.ip.id=getpid();        /* 16-bit ID field */
packet.ip.frag_off=0;         /* 13-bit Fragment offset */
packet.ip.ttl=255;           /* 8-bit Time to Live */
packet.ip.protocol=IPPROTO_TCP; /* 8-bit Protocol */
packet.ip.check=0;           /* 16-bit Header checksum (filled in below) */
packet.ip.saddr=saddr;       /* 32-bit Source Address */
packet.ip.daddr=daddr;       /* 32-bit Destination Address */
```

As the following code fragment shows, this technique even uses an error-checking routine to make sure the address chosen is routable to, but not active. When the attacker enters an address, the attack code pings the address (notice the slickping line in the following code fragment) to ensure it meets these requirements. If the address is active, it sends a RESET when it receives the SYN/ACK for the system under attack. When the target system receives the RESET, it releases the memory and decrements the service queue counter, rendering the attack ineffective. From an intrusion-detection stand-point, these bogus packets assembled for the purpose of attacking and probing can be called crafted packets. Quite often the authors of software that crafts packets make a small error at some point, or take a shortcut, and this gives the packet a unique signature. You can use these signatures in intrusion detection. When you detect evidence of a crafted packet, you know the sender is up to something.

case 3:

```
if(!optflags[1]){
    fprintf(stderr,"Enter a host
    first\n");
    usleep(MENUSLEEP);
    break;
}
```

```
/* Raw ICMP socket */
```

```
if((sock2=socket(AF_INET,SOCK_RAW,IPPROTO_ICMP))<0{
    perror("\nHmmm.... socket
    problems\n");
    exit(1);
}
printf("[number of ICMP_ECHO's]-> ");
fgets(tmp,MENUBUF,stdin);
if(!(icmpAmt=atoi(tmp)))break;
if(slickping(icmpAmt,sock2,unreach)){
    fprintf(stderr,"Host is reachable...
    Pick a new one\n");
    sleep(1);
```

Now you have a technique to use as a generic denial of service; you hit a target system with SYNs until it cannot speak (establish new connections). Systems vulnerable to this attack can be kept out of service until the attacker decides to go away and SYN no more. In the Mitnick attack, the goal was to silence one side of a TCP connection and masquerade as the silenced, trusted party.

Identifying Trust Relationships

So how did Mitnick identify which systems to silence? How did he confirm a trust relationship existed? It turns out that many complex attacks are preceded by intelligence gathering techniques, or recon probes. Here are the recon probes detected by TCPdump, a network monitoring tool developed by the Department of Energy's Lawrence Livermore Lab, and reported in Tsutomu's post.

"The IP spoofing attack started at about 14:09:32 PST on 12/25/94. The first probes were from toad.com." (This information was derived from packet logs.)

```
14:09:32 toad.com# finger -l @target
14:10:21 toad.com# finger -l @server
14:10:50 toad.com# finger -l root@server
14:11:07 toad.com# finger -l @x-terminal
14:11:38 toad.com# showmount -e x-terminal
14:11:49 toad.com# rpcinfo -p x-terminal
14:12:05 toad.com# finger -l root@x-terminal
```

Each of the commands shown, `finger`, `showmount`, and `rpcinfo` can provide information about UNIX systems. If you work in a UNIX environment and haven't experimented with these commands in a long while, it may be worthwhile to substitute some of your machine names for `target`, `server`, and `x-terminal` to see what you can learn.

—> **finger tells you who is logged on to the system, when they**

logged on, when they last logged on, where they are logging on from, how long they have been idle, whether they have mail, and when their birthday is (well, scratch the birthday). The analogous command for MS Windows systems is NBTSTAT

—> showmount -e provides information about the file systems mounted with Network File System (NFS). Of particular interest to attackers are file systems that are mounted world reachable or writable (that is, available to everyone).

—> rpcinfo provides information about the remote procedure call services available on a system. rpcinfo -p gives the port where these services reside.

These days most sites block TCP port 79 (finger) at their firewall or filtering router, but it might be a good idea to try this from your home ISP account; get permission first! Again, hopefully your site blocks TCP/UDP port 111 (portmapper), but this is worth testing as well. In recent years, so-called secure portmappers have become available either from vendors or as an external package developed by Wietse Venema, available from the Coast archive at ftp://coast.cs.purdue.edu/pub.

We are looking for stories for our next issue. If you want to share more material about C, C++, PHP, Intrusion Detection, Honeypots or Honeynets, submit an article by the date below. Make sure you have AO Newsletter in the subject line. Submit to msmittens@msmittens.com by Friday January 10, 2003.

Number Conversion

by MrLeachy

well here is my first (and i hope not last) tut on AntiOnline

how to convert between various numbering systems:

i'll start by going from base 2 (binary) to assorted other formats and will add more as i go

base 2 (binary)—> base 16 (hex)

as we all know, binary uses 1's and 0's to represent numbers, and hex uses numbers from 0 - 9 and letters from A - F

binary (2)	hex (16)	decimal (10)	octal (8)
0000	0	0	0
0001	1	1	1
0010	2	2	2
0011	3	3	3
0100	4	4	4
0101	5	5	5
0110	6	6	6
0111	7	7	7
1000	8	8	
1001	9	9	
1010	A	10	
1011	B	11	
1100	C	12	
1101	D	13	
1110	E	14	
1111	F	15	

to go from binary to hex, get your binary number e.g. 1111 0111
split it into groups of four digits, if you get a group which isnt four digits, add 0's to the right side until it is 4 digits long

now back to our example 1111 0111 becomes F7 according to the above table

to go from hex to binary, simply refer to the above conversion chart and reverse the above procedure:
ie F becomes 1111 and 7 becomes 0111

to convert hex to decimal we do this:
use the hex number codes to correspond them to decimal numbers ie f is 15, 7

is 7 etc

and reading from right to left in powers of 16 starting from 16^0 , 16^1
etc

so F7 becomes $(F \times 16^1) + (7 \times 16^0)$

—> $(F \times 16) + 7$

—> 247 decimal

to convert decimal to hex, the easiest way i know of is to convert to binary
and then convert to the hex numbers using the conversion chart above

To make our original binary number octal, we just split the binary number
into groups of 3 instead of 4

so 11110111

is split to 111 101 011 (hope that is right)

then you convert your groups of 3 binary numbers to their corresponding
octal's

so 111 101 011 becomes:

753

to convert octal to binary, you simply reverse the above procedure and add
zero's to the left side of any odd groups

Octal to decimal uses the same idea as converting decimal to hex, convert
your octal to binary, then convert the binary number to decimal

any other parts i may have missed can be done using the above ideas and the
conversion chart above, hope this is of help to someone out there

MrLeachy