# CS547A Homework set #4

**Due Monday November, 10 2003 in class at 13:30**

**Exercises (from Stinson's book)**

## 3.3, 3.5, 3.6. (you may use Maple if you like)

## Other Exercises

## Pseudo-Random Permutation Generator

We say that $\{ \pi_k : \{0,1\}^n \to \{0,1\}^n \}_k$ is a *Pseudo-Random Permutation Generator* (PRPG) if it is a PRG and each $\pi_k$ is a permutation (a one-to-one function). Consider the following family of permutations $\{ \pi_k : \{0,1\}^{2n} \to \{0,1\}^{2n} \}_k$ defined from a Pseudo-Random Function Generator $\{ f_k : \{0,1\}^n \to \{0,1\}^n \}_k$:

$$\pi_k(x,y) = [\, y \,,\, x \oplus f_k(y) \,]$$

(a) Show that $\pi_k(x,y)$ is indeed a permutation (a one-to-one function).

Define similarly

$$\pi_{k1,k2}(x,y) = \pi_{k1}(\pi_{k2}(x,y)) \quad \text{AND} \quad \pi_{k1,k2,k3}(x,y) = \pi_{k1}(\pi_{k2}(\pi_{k3}(x,y)))$$

It has been proven that $\{ \pi_{k1,k2,k3}(x,y): \{0,1\}^{2n} \to \{0,1\}^{2n} \}_{k1,k2,k3}$ is a PRPG.
(I am not asking you to prove this because it is too difficult…)

(b) Show that $\{ \pi_k : \{0,1\}^{2n} \to \{0,1\}^{2n} \}_k$ is not a PRPG.

(c) Show that $\{ \pi_{k1,k2} : \{0,1\}^{2n} \to \{0,1\}^{2n} \}_{k1,k2}$ is not a PRPG.

(d) Explain the relationship between these permutations and DES.

(e) Show how to compute their inverses $\pi^{-1}_k(x,y)$, $\pi^{-1}_{k1,k2}(x,y)$, $\pi^{-1}_{k1,k2,k3}(x,y)$.

(f) Explain how Alice and Bob could share a secret key and use both $\pi$ and $\pi^{-1}$ to do encryption/decryption of bit-strings of size 2n. What would be the security properties of such a system ? (Make the strongest possible statement and justify it: 1.ciphertext only, 2.known plaintext, 3.chosen plaintext, 4.known ciphertext, 5.chosen ciphertext. Possible answers are "not even 1.", "1. but not 2.", "2. but not 3.", "3. but not 4.", "4. but not 5.", or "5.").

(g) Show that if the plaintext messages contain some redundancy then the messages encrypted by this system are automatically authenticated.

*More on back*

## Factoring

(1) Let **n=p*q**, the product of two primes, such that **p>q**.
Show that if $\sqrt{p}-\sqrt{q} < \sqrt{2}$ then $\lfloor\sqrt{n}\rfloor = (p+q)/2$.

(2) Deduce from (a) an efficient algorithm to factor RSA modulus **(n=p*q)** for which $\sqrt{p}-\sqrt{q} < \sqrt{2}$.

(3) Generalize this factoring method using products of the form $\lfloor\sqrt{kn}\rfloor=(ap+bq)/2$ for **n=p*q** and **k=a*b** for known **a,b**.

## MAPLE™.

THE GREAT 2003 FACTORING CONTEST

Let

**n:=20122319630229216921962298483056313350698743555701429334232725725303350016549558812616741122199920737484727776834783698257649430894364938640682714094653493954623828038293513946779387194280813566001099175450551623452261932231802416253337889371 7**

**a)** find two primes **p,q** such that **n=p*q** and **|p|≈|q|≈120** digits.

## Block Cipher Modes of Operations

Consider the following pieces of MAPLE™ code that define an encryption function “enc” and a decryption function “dec” for messages of 64 bits:

```
> with(numtheory):
> enc:= (p,e,m) -> m&^e mod p;
> dec:= (p,e,c) -> c&^(e^(-1) mod (p-1)) mod p;
> p:=nextprime(2^64+1000027);
> e:=16755434444356788983;
```

**b)** Use the above statements as a block cipher and implement three MAPLE™ procedures to encrypt/decrypt/authenticate lists of messages using the CBC mode of operation:

```
> CBC_enc:=proc(IV,LIST)…
> CBC_dec:=proc(IV,LIST)…
> CBC_mac:=proc(IV,LIST)…
```

Where LIST is a MAPLE™ list of numbers, and IV is an integer between 0 and $2^{64}$-1. Note that in the CBC_enc mode, you are encouraged to use a random first plaintext block to randomnize the encryption of the entire list. You may ignore this block at decryption.

**c)** Encrypt, Encrypt and Authenticate, Encrypt and Decrypt, the following list using your student number as IV.

**[2,7182818, 2845904523, 53, 6028, 747135, 2662, 497757,51]**