Dr. A. Betten Fall 2005

M360 Mathematics of Information Security

exercise sheet # 2

Exercise # 1 (5 points)

Decipher the following shift cipher message:

ndf clyvd lxzyr mpde fytgpcdtetpd

You may use the following maple code:

```
with(StringTools):
caesar := proc(s::string, shift::integer)
  local S, l, i, c;
  S := convert(s,'bytes');
  l := nops(S);
  for i to l do
    c := S[i];
    if c >= 97 and c <= 122 then
      c := c - 97 + shift;
      c := irem(c, 26);
      if c < 0 then c := c + 26; end;
      S[i] := 97 + c;
    end;
  end;
  return convert(S,'bytes');
end;
```

Exercise # 2 (5 points)

Let $a, b, c, d, k \in \mathbb{Z}$, $n \in \mathbb{N} \setminus \{0\}$. If $a \equiv b \bmod n$ and $c \equiv d \bmod n$, then show that

a) $a + c \equiv b + d \bmod n$

b) $ac \equiv bd \bmod n$

c) $a + k \equiv b + k \bmod n$

d) $ak \equiv bk \bmod n$.

due to Friday, 9/9/05.