Section 4.6

Ex. 8.

In the ciphertext, "V" occurs many times, so we can guess it shift $22-5=17$ from "E" to "V", so the original plaintext is:

"Men Love to wonder, and that is the seed of science."

Ex. 14.

"GRIZZ LYBEA RSXXX" → "IZGZR BELAY XXRXS"

$\sigma(1)=3,\ \sigma(2)=5,\ \sigma(3)=1,\ \sigma(4)=2,\ \sigma(5)=4$

Ex. 26.

The inverse of $e=17 \pmod{52\cdot60}$ is $d=2753$

then:

$3185^{2753} \bmod 53\cdot61 = 1816$

$2038^{2753} \bmod 53\cdot61 = 2008$

$2466^{2753} \bmod 53\cdot61 = 1717$

$2550^{2753} \bmod 53\cdot61 = 0411$

⇒ So the original message is "RSQUIRREL"

Ex. 30

Alice sends $2^7 \bmod 101 = 27$ to Bob

Bod sends $2^9 \bmod 101 = 7$ to Alice

so: Alice computes: $7^7 \bmod 101 = 90$

Bob computes: $27^9 \bmod 101 = 90$

So the shared key is 90.

Ex. 32.

"BUY NOW" → "0120 2413 1422"

Step 1:

$0120^{183} \bmod 2867 = 1665$

$2413^{183} \bmod 2867 = 1728$

$1422^{183} \bmod 2867 = 2123$

→ "1665 1728 2123"

Step 2:

$1665^{21} \bmod 3127 = 2806$

$1728^{21} \bmod 3127 = 1327$

$2123^{21} \bmod 3127 = 0412$

→ "2806 1327 0412"