8.3 Exponentiation Ciphers;

We will now study a Cipher based on Fast Modular Exponentiation. This was invented in 1978 by Pohlig and Hellmann. This Cryptosystem is more resistant to Cryptoanalysis.

Let $p$ be an odd prime and let $e$ be a positive integer such that $(e, p-1) = 1$. This integer $e$ will be used as an encryption key.

Procedure for encryption: Assign a two digit number to every letter by placing a zero at the beginning for letters which have their numbers between 0 and 10. Thus: $A \leftarrow 00$, $B \leftarrow 01$, ..., $T \leftarrow 09$, $K \leftarrow 10$, etc.

Next, the resulting numbers are divided into blocks of $2m$ decimal digits, where $m$ is chosen as follows.

The entire block of numerical equivalent corresponding to $m$ letters, which gives an integer with $2m$ decimal digits, are less than $p$, the odd prime mentioned above.

For Example: $A$ $B$ $C$ $\ldots$ $\ldots$ $Z$

$$00 \ 01 \ 02 \ \ldots \ \ldots \ 25$$

$$\frac{25 \ 25 \ \ldots \ 25}{m \ times} < p < \frac{25 \ 25 \ \ldots \ 25}{(m+1) \ times}$$
For example, suppose \( p = 4283 \). Then \( m = 2 \) works, since
\[
\frac{2525}{m=2} < p < \frac{252525}{m=3}
\]
If \( p = 670417 \), then \( m = 3 \) since
\[
\frac{252525}{m=3} < 670417 < \frac{25252525}{m=4}
\]
In the first example, the text is broken into blocks of two letters (since \( m = 2 \)) and for the second choice of \( p \), we have blocks of three letters, since \( m = 3 \). The reason this is done is to ensure that the blocks are unique modulo \( p \).

Encryption Step: A block \( A \) is encoded using the transformation
\[
C = A^e \mod p
\]
Here \( A \) denotes a block of the plaintext and \( C \) is the encoded ciphertext. The ciphertext \( C \) is an integer satisfying \( 0 \leq C < p \), and this is the integer in ciphertext. Note that the ciphertext will be blocks of \( 2m \) integers.
Eg: We send the message
WAIT UNTIL THE SUN SHINES NELLIE
using the pair \( p = 2819 \) and \( e = 23 \).
Note that \( (e, p-1) = (23, 2818) = 1 \). We have
\[
2525 < 2819 < 252525.
\]
Hence the block size \( m = 2 \), so each block has \( 2m = 4 \) numbers.

Add an \( X \) at the end of the plain text to fill out the final block of four digits. In this example, the number of letters in the text is 27, so we add an \( X \) at the end to get blocks of size 2.

WA 17 UN TI LT HE SU
2200 0819 2013 1908 1119 0704 1820

1318 0708 1304 1813 0411 1108 0423
NS HI NE SN E'L LI E8

Here we then write the corresponding numbers in blocks of 4. Example
WA : 2200, where W \( \rightarrow \) 22, A \( \rightarrow \) 00.
NS : 1318, where N \( \rightarrow \) 13, S \( \rightarrow \) 18.

Encode using the formula \( C \equiv p^{e} \mod 2819 \).
Eg: NA \( \rightarrow \) 2200

How do we encode AN? Do \( C = 2200? \)
Since \( (2819, 23) = 1 \), we find \( (23, 2573) - (21, 2818) = 1 \).
Hence $2573$ is the modular inverse of $23$ modulo $2818$. This will be used in decryption.

Let us continue with encryption.

For $P = 2200$, we find using

$$C ≡ P^{23} \mod 2819,$$

using modular exponentiation,

$$(2200)^{23} ≡ 602 \mod 2819.$$  

This step is typically done using computer calculation.

Continuing in this manner, we get the ciphertext numbers to be

$$C: 602 \quad 2242 \quad 1007 \quad 439 \quad 2612$$
$$\quad 280 \quad 1303 \quad 1981 \quad 1511 \quad 1981$$
$$\quad 233 \quad 1013 \quad 274 \quad 540.$$  

This will be the encrypted ciphertext in numbers.

To decrypt, we will use the fact that $2573$ is the modular inverse of $23$ modulo $2818$. 