Continuing with the encryption and decryption protocols, we discussed the case of Caesar Cipher. Let us briefly recall that.

Let $P$ be the Plain text message and $C$ the Cipher text message. Encryption is given by the rule

$$C \equiv P + 3 \mod 26$$

and Decryption is given by the rule

$$P \equiv C - 3 \mod 26.$$ 

Here $k = 3$ is called the Caesar Key, $C$ and $P$ can take the values between 0 and 25, both inclusive.

**SHIFT TRANSFORMATIONS**

More generally, we can also consider transformations of the form

$$C \equiv P + k \mod 26,$$

where the encryption key $k$ can be any integer. These form the general class of *shift transformations*, of which the Caesar Cipher is a special case. Of course, the decryption rule is given by

$$P \equiv C + k \mod 26.$$

As an example, let us consider the Shift Transformation

$$C \equiv P + 17 \mod 26.$$ 

So the encryption key in the shift transformation is 17. Let us encrypt the plain text message

**THOMAS JEFFERSON LIVES**

The first step is the same as in the Caesar Cipher, namely we note down the corresponding number between 0 and 25 assigned to the letters in the test. So we have
Applying \( C \equiv P + 17 \mod 26 \), we get the following numbers, to which we then assign the corresponding letters; for example \( 19 \rightarrow 19 + 17 \mod 26 \), which is equal to 10. Thus we get

\[
C: \quad 10 \quad 24 \quad 5 \quad 3 \quad 17 \quad 9 \quad 0 \quad 21 \quad 22 \quad 22 \quad 21 \quad 8 \quad 9 \quad 5 \quad 4 \quad 2 \quad 25 \quad 12 \quad 21 \quad 9
\]

The Cipher text is then grouped into blocks of five letters so it reads

\[
K Y F D R J A V W W V I J F E C Z M V J:
\]

Suppose that we wish to decipher the ciphertext \( C \) below

\[
URUTM \quad HQEQQ \quad ZMXUF \quad FXQRM \quad DFTQD
\]

which has been encrypted using a shift transformation with key \( k = 12 \), and the ciphertext has been divided in to blocks of five letters. We next assign the numbers to the letters in the cipher text, we get

\[
20 \quad 17 \quad 20 \quad 19 \quad 12 \quad 7 \quad 16 \quad 4 \quad 16 \quad 16 \quad 25 \quad 12 \quad 23 \quad 20 \quad 5 \quad 5 \quad 23 \quad 16 \quad 17 \quad 12 \quad 3 \quad 5 \quad 19 \quad 16 \quad 3.
\]

In other words,

\[
URUTM \quad : \quad 20, 17, 20, 19, 12 \\
HQEQQ \quad : \quad 7, 16, 4, 16, 16 \\
ZMXUF \quad : \quad 25, 12, 23, 20, 5 \\
FXQRM \quad : \quad 5, 23, 16, 17, 12 \\
DFTQD \quad : \quad 3, 5, 19, 16, 3.
\]

The plaintext \( P \) is then obtained by

\[
P \equiv C - 12 \mod 26.
\]

For example \( 20 \mapsto (20 - 12) \mod 26 \), thus \( 20 \mapsto 8 \), and \( 7 \mapsto -5 \mod 26 \) and \(-5 \equiv 21 \mod 26 \), and so \( 7 \mapsto 21 \), since all the values should lie between 0 and 25, both included. We thus get the following numbers to which the corresponding letters are assigned:

\[
8 \quad 5 \quad 8 \quad 7 \quad 0 \quad 21 \quad 14 \quad 18 \quad 4 \quad 4 \quad 13 \quad 0 \quad 11 \quad 8 \quad 19 \quad 19 \quad 11 \quad 4 \quad 5 \quad 0 \quad 17 \quad 19 \quad 7 \quad 4 \quad 17.
\]

Now assigning the corresponding letters, we get
IFIHA VESEE NALIT TLEFA RTHEN
and so the Plaintext P reads

IF I HAVE SEEN A LITTLE FARThER.
**Affine Transformations:**

The encryption in the case of affine transformations is given by the general formula

\[ C \equiv aP + b \mod 26; \ a, b \in \mathbb{Z}. \]

Suppose the plain text P is

THE EARL OF OXFORD.

The corresponding numbers are

19 7 4 4 0 7 11 14 5 14 23 5 14 17 3.

Let \( a = 5 \) and \( b = 8 \). We should apply the encryption \( C \equiv 5P + 8 \mod 26 \). Thus for example, the number 19 assigned in the plain text is sent to the number \((5.19 + 8) \mod 26\). Hence

\[ 19 \mapsto (5.19 + 8) \mod 26 = 103 \mod 26 = 25 \mod 26. \]

Continuing in this manner, the above numbers get transformed to

25 17 2 2 8 15 11 0 7 0 19 7 0 15 23.

The corresponding letters are

ZRCCIPLAHATHAPX

which is then grouped in to blocks of five. So the cipher text C reads

ZRCCI PLAHA THAPX.

**Decrypting Ciphertext for Affine Transformations:**

Since an affine transformation is given by a formula

\[ C \equiv aP + b; \ a, b \in \mathbb{Z}, \]

the decryption process is a little more involved. The aim is to express the plaintext \( P \) in terms of the ciphertext \( C \). Note first that we get

\[ aP \equiv (C - b) \mod 26. \]

To get \( P \) on the left hand side of this congruence, we need to multiply both sides of the congruence by the modular inverse \( \bar{a} \) of \( a \) modulo 26. We then get

\[ P \equiv \bar{a}(C - b) \mod 26. \]
where $a.a \equiv 1 \mod 26$.

For example, suppose the affine transformation is
\[ C \equiv 21P + 5 \mod 26. \]

Here $a = 21$ and $b = 5$. The modular inverse of 21 modulo 26 is 5, since $5.21 = 105 \equiv 1 \mod 26$. Hence $\bar{a} = 5$ and $\bar{a}(C - b)$ becomes $5(C - 5)$.

\[ P \equiv 5(C - 5) \equiv 5C - 25 \equiv 5C + 1 \mod 26, \]

since $-25$ is congruent to 1 modulo 26.

Suppose the cipher text $C$ obtained using the affine transformation $C \equiv 21P + 5 \mod 26$ is as below.

\[ \text{YLFQK PCRIT} \]

As before, we first assign the numbers to these letters. This gives us

\[ 24 \ 11 \ 5 \ 16 \ 10 \ \ 24 \ 11 \ 8 \ 15 \ 18. \]

To decrypt, we should use the transformation $P \equiv 5C + 1 \mod 26$. Thus for example, the number 24 in the ciphertext corresponds to the letter $(5.24 + 1)$ modulo 26, which is 121 modulo 26, which is 17, since $121 = 104 + 17 = (4.26) + 17$. Thus the corresponding numbers we get using this formula are

\[ 17 \ 4 \ 0 \ 3 \ 12 \ 24 \ 11 \ 8 \ 15 \ 18. \]

Then the corresponding letters in the plain text are

\[ \text{READMYLIPS} \]

and so the plaintext message is READ MY LIPS.

**BRIEF OVERVIEW OF CRYPTANALYSIS:**

In this section, we give a very brief outline of techniques used in cryptanalysis, which is the term used to breaking secrecy systems. This decoding is language specific and uses particularities of the language and also involves some guesswork. For instance, a plain text in English language would have words that always have vowels. There are also some short words that are frequently used like The, is, as, it, to, etc. The decoding is greatly aided if one knows the kind of encryption, i.e. shift transformation or affine transformation, used to get the ciphertext. The exact transformation equation can then be written after pinning down some of the deciphered letters that occur frequently. This helps validate the guess work. After pinning down some of the deciphered letters followed by validation, one can write down the exact congruence equations that gives the precise encryption transformation.
NOTE: Please note that this is just an overview and will not be discussed in detail. This part on Cryptanalysis will not be examined in the final exam.

We end this lecture by revising some previous material and working out some problems.

For a fixed $a > 1$, let $F(a)$ for the set of positive integers $n$ satisfying $a^{n-1} \equiv 1 \mod n$. By Fermat’s theorem, $F(a)$ includes all primes that are not divisors of $a$. If $n \in F(a)$, then the gcd$(a, n) = 1$, since clearly the gcd $(a^{n-1}, n) = 1$. Also, $a^n \equiv a \mod n$ and the reverse implication is true provided that $a$ and $n$ are coprime.

Note that a composite number $n$ belonging to $F(a)$ is a pseudoprime to base $a$.

Q 1. Suppose for some $m$ we have that $n$ divides $a^{m-1}$ and $n \equiv 1 \mod m$. Then show that $n \in F(a)$.

Ans: We have $a^m \equiv 1 \mod n$, and that $n - 1$ is a multiple of $m$. Hence $a^{n-1} \equiv 1 \mod n$.

Examples: $2^{11} - 1 = 2047 = 23 \times 89$, both 23 and 89 are congruent to 1 mod 11. So 2047 is 2-pseudoprime.

$3^6 - 1 = 26 \times 28 = 2^3 \times 7 \times 13$. Hence $7 \times 13 = 91$ is a 3-pseudoprime.