FIT5163 Information & Computer Security
Discussion Sheet 2
Foundations of Cryptography

1. What characteristics would make an encryption absolutely unbreakable? What characteristics would make an encryption impractical to break?

   Absolutely unbreakable: unpredictable randomness.
   Impractical: work factor.

2. Does a substitution need to be a permutation of the plaintext symbols? Why or why not?

   No. A substitution can be to an entirely different alphabet. (As an example, read the Arthur Conan Doyle Sherlock Holmes Case of the Dancing Men.) One plaintext symbol can convert to several ciphertext symbols, or vice versa. For example, Morse code is a form of substitution of alphabetic letters to dots and dashes. Two plaintext characters could map the same ciphertext character as long as the recipient could distinguish between the two.

3. Explain why the product of two relatively simple ciphers, such as a substitution and a transposition, can achieve a high degree of security.

   Each cipher contributes its own strength, so ideally the strength of the product is at least the product of the strengths of the input ciphers. A substitution cipher contributes confusion, whereas a transposition performs diffusion. The DES and AES algorithms both use a combination of relatively simple functions. Obviously, however, just composing two ciphers is not guaranteed to result in a stronger combination.

4. DES and AES are both "turn the handle" algorithms in that they use repetition of some number of very similar cycles. What are the advantages (to implementer, users, cryptanalysts, etc.) of this approach?

   Implementers like this approach, because it usually leads to compact and fast implementations. Small, simple implementations can be embedded in firmware or on smart cards, for example.
   Users like these algorithms because they tend to be fast in execution.
   Cryptanalysts like the simple structure because they can trace the diffusion of bits through the output.

5. What is the difference between block cipher and stream cipher?

   A stream cipher is one that encrypts a digital data stream one bit or one byte at a time. A block cipher is one in which a block of plaintext is treated as a whole and used to produce a ciphertext block of equal length.

6. What is the difference between an unconditionally secure cipher and a computationally secure cipher?

   An encryption scheme is unconditionally secure if the ciphertext generated by the scheme does not contain enough information to determine uniquely the corresponding plaintext, no matter how much ciphertext is available. An encryption scheme is said to be computationally secure if:
   1) the cost of breaking the cipher exceeds the value of the encrypted information, and
   2) the time required to break the cipher exceeds the useful lifetime of the information.

7. What do you mean by monoalphabetic cipher and polyalphabetic cipher and what are the difference(s)?

A monoalphabetic substitution cipher maps a plaintext alphabet to a ciphertext alphabet, so that each letter of the plaintext alphabet maps to a single unique letter of the ciphertext alphabet. A polyalphabetic substitution cipher uses a separate monoalphabetic substitution cipher for each successive letter of plaintext, depending on a key.

8. Consider the Encryption and Decryption table for Substitution Cipher.

Encryption		**Decryption**	
Plaintext	Ciphertext	Ciphertext	Plaintext
0000	1110	0000	1110
0001	0100	0001	0011
0010	1101	0010	0100
0011	0001	0011	1000
0100	0010	0100	0001
0101	1111	0101	1100
0110	1011	0110	1010
0111	1000	0111	1111
1000	0011	1000	0111
1001	1010	1001	1101
1010	0110	1010	1001
1011	1100	1011	0110
1100	0101	1100	1011
1101	1001	1101	0010
1110	0000	1110	0000
1111	0111	1111	0101

Is it practical to use the above substitution cipher? Give reasons.

In the case of an arbitrary reversible cipher as shown in the table shown above, if a small block size, such as $n = 4$, is used, then the system is equivalent to a classical substitution cipher. For small n, such systems are vulnerable to a statistical analysis of the plaintext. This weakness is not inherent in the use of substitution cipher but rather results from the use of a small block size. If n is sufficiently large and an arbitrary reversible substitution between plaintext and ciphertext is allowed, then the statistical characteristics of the plaintext are masked to such an extent that this type of cryptanalysis is not feasible. In this table the unique mapping which shows the value of ciphertext for each plaintext is the key. In general, for an n-bit ideal block, the length of the key defined in this manner is $n \times 2^n$. For $n = 4, key\ length = n \times 2^n = 4 \times 2^4 = 4 \times 16 = 64$. But for large n, $length of key = n \times 2^n$ makes the system impractical to cryptanalyse.

9. The function P is defined as: $P : \{0, \ldots, 2^{32} - 1\} \rightarrow \{0, \ldots, 2^{32} - 1\}$ where the value of $y = P(x)$ is based on a fixed shuffling of x bits as shown in Figure 1:

$x \quad y$
$b_{16} \rightarrow b_1$
$b_7 \rightarrow b_2$
$b_{20} \rightarrow b_3$
$b_{21} \rightarrow b_4$
$b_{29} \rightarrow b_5$
$b_{12} \rightarrow b_6$
$b_{28} \rightarrow b_7$
$b_{17} \rightarrow b_8$
$b_1 \rightarrow b_9$
$b_{15} \rightarrow b_{10}$
$b_{23} \rightarrow b_{11}$
$b_{26} \rightarrow b_{12}$

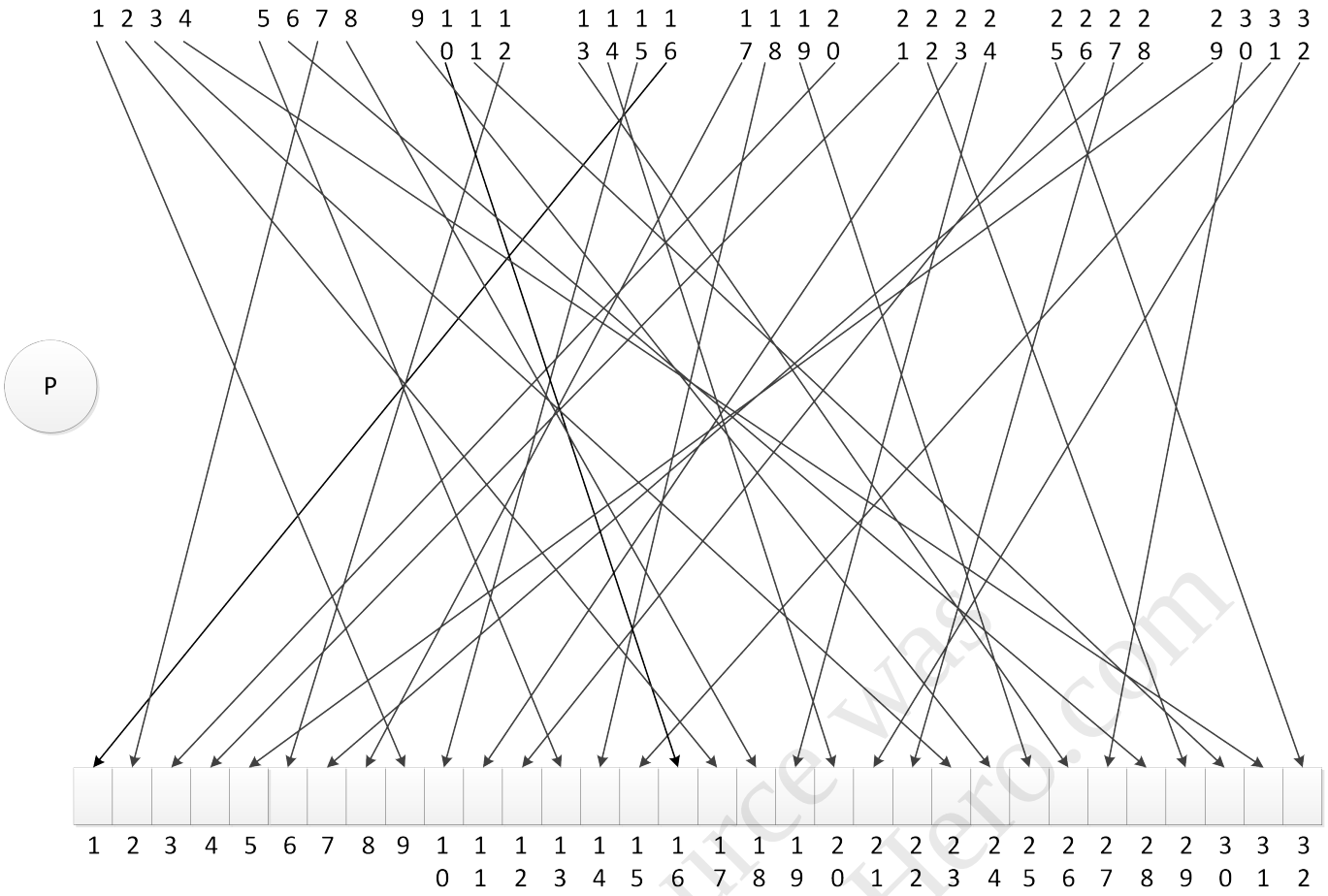

Figure 1: The P function

$b_5 \rightarrow b_{13}$
$b_{18} \rightarrow b_{14}$
$b_{31} \rightarrow b_{15}$
$b_{10} \rightarrow b_{16}$
$b_2 \rightarrow b_{17}$
$b_8 \rightarrow b_{18}$
$b_{24} \rightarrow b_{19}$
$b_{14} \rightarrow b_{20}$
$b_{32} \rightarrow b_{21}$
$b_{27} \rightarrow b_{22}$
$b_3 \rightarrow b_{23}$
$b_9 \rightarrow b_{24}$
$b_{19} \rightarrow b_{25}$
$b_{13} \rightarrow b_{26}$
$b_{30} \rightarrow b_{27}$
$b_6 \rightarrow b_{28}$
$b_{22} \rightarrow b_{29}$
$b_{11} \rightarrow b_{30}$
$b_4 \rightarrow b_{31}$
$b_{25} \rightarrow b_{32}$

(a) For $x = FF00FF00$ determine the value of y's following bits:

- b_{11} =1
- b_{23} =1

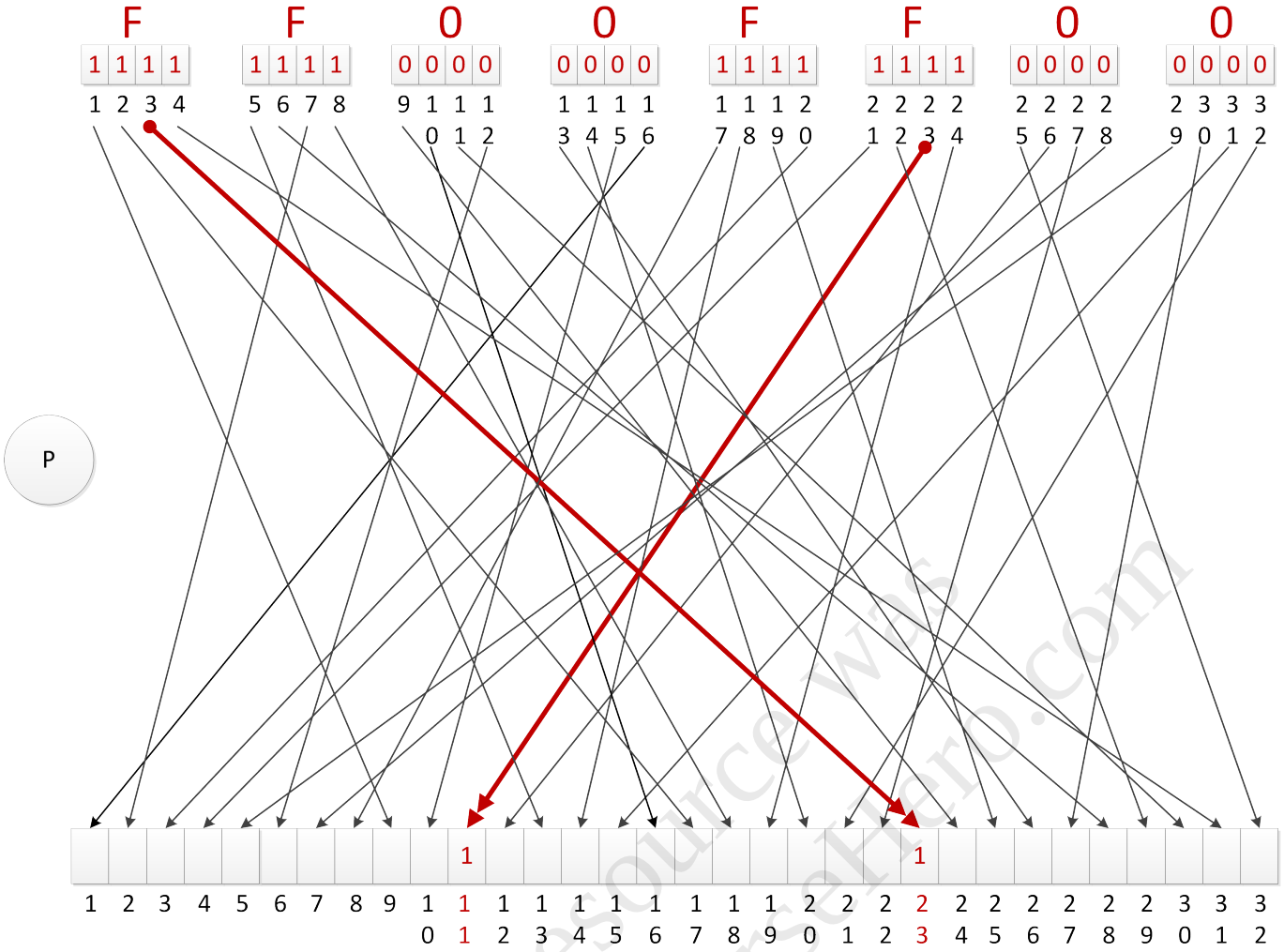

Figure 2: The output of P function for bits b_{11} and b_{23}

For $x = FF00FF00$ $y = 71ACE29A$

(b) For the following values of x determine the value of y:

- $x = FFFFFFFF$
  $y = FFFFFFFF$
- $x = 00000000$
  $y = 00000000$
- $x = F0000000$
  as only the first four bit are one we can determine where these bits are located in the output: $x(b_1) \rightarrow y(b_9)$, $x(b_2) \rightarrow y(b_{17})$, $x(b_3) \rightarrow y(b_{23})$, and $x(b_4) \rightarrow y(b_{31})$ hence the binary output is as follows:
  0000 0000 1000 0000 1000 0010 0000 0010 and the hex: $y = 00808202$

10. Define and distinguish between the terms diffusion and confusion (with respect to encryption).

In diffusion, the statistical structure of the plaintext is dissipated into long range statistics of the ciphertext. This is achieved by having each plaintext digit affect the value of many ciphertext digits, which is equivalent to saying that each ciphertext digit is affected by many plaintext digits. Confusion seeks to make the relationship between the statistics of the ciphertext and the value of the encryption key as complex as possible, again to thwart attempts to discover the key. Thus, even if the attacker can get some handle on the statistics of the ciphertext, the way in which the key was used to produce that ciphertext is so complex as to make it difficult to deduce the key. This is achieved by the use of a complex substitution algorithm.

11. Explain the avalanche effect.

    The avalanche effect is a property of any encryption algorithm such that a small change in either the plaintext or the key produces a significant change in the ciphertext.

12. With regard to Playfair cipher perform the following:

    (a) Construct a Playfair matrix with the key: `largest`.

L	A	R	G	E
S	T	B	C	D
F	H	I/J	K	M
N	O	P	Q	U
V	W	X	Y	Z

    (b) Using the matrix encrypt the message:
    `Must see you over Cadogan West.  Coming at once.`
    `MU ST SE EY OU OV ER CA DO GA NW ES TC OM IN GA TO NC EX`
    `UZ TB DL GZ PN NW LG TG TU ER OV LD BD UH FP ER HW QS RZ`

13. Regarding Playfair cipher answer the following questions:

    (a) How many possible keys does the Playfair cipher have? Ignore the fact that some keys might produce identical encryption results. Express your answer as an approximate power of 2.
    $25! \approx 2^{84}$
    In general, there are $n!$ permutations of a set of n elements. First element can be chosen in n ways, second in $n-1$ ways, third in $n-2$ ways and so on.

    (b) Now take into account the fact that some Playfair keys produce the same encryption results. How many effectively unique keys does the Playfair cipher have?
    Given any 5×5 configuration, any of the four row rotations is equivalent, for a total of five equivalent configurations. (Rotation of the row does not change the relative position of the letters in a row for the ciphertext.) For each of these five configurations, any of the four column rotations is equivalent. So each configuration in fact represents 25 equivalent configurations. Thus, the total number of unique keys is $\frac{25!}{25} = 24!$

14. Using the Vigenère cipher, encrypt the word *explanation* using the key *leg*.

key:	`legleglegle`	11	4	6	11	4	6	11	4	6	11	4
plaintext:	`explanation`	4	23	15	11	0	13	0	19	8	14	13
ciphertext:	`PBVWETLXOZR`	15	1	21	22	4	19	11	23	14	25	17

$C = (p + k) \; mod \; 26$