Basics of Cryptology

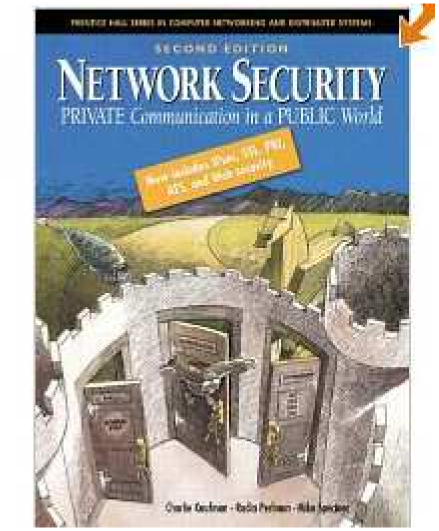
Book and lecture notes

- Book:

  Network Security: Private Communication in a Public World (2nd Edition)

  C. Kaufman, R. Perlman, and M. Speciner

  Prentice Hall, 2002



- For this part, you can study on the lecture notes

Introduction: let us start with a story

- It was a dark and stormy night.
- A shiny object caught Alice's eye. A diamond cufflink!
- Only one person in the household could afford diamond cufflinks! So it was the butler, after all!
- Alice had to warn Bob. But how could she get a message to him without alerting the butler?
- If she phoned Bob, the butler might listen on an extension. If she sent a carrier pigeon out the window with the message taped to its foot, how would Bob know it was Alice that was sending the message and not Trudy attempting to frame the butler because he spurned her advances?

Introduction

- That is what this part of the course is about. We do discuss how to communicate securely over an insecure medium.
- What do we mean by communicating securely?

  Alice should be able to send a message to Bob that only Bob can understand, even though Alice can't avoid having others see what she sends. When Bob receives a message, he should be able to know for certain that it was Alice who sent the message, and that nobody tampered with the contents of the message in the time between when Alice launched the message and Bob received it.
- What do we mean by an insecure medium?

  In some dictionary or another, under the definition of "insecure medium" should be a picture of the *Internet*. In the current world most (all) the computers are interconnected, and people talk about connecting household appliances as well, all into some wonderful global internetwork. How wonderful! You'd be able to send electronic mail to anyone in the world. You'd also be able to control your nuclear power plant with simple commands sent across the network while you were vacationing in Fiji. Or some Mediterranean islands.

  Inside the network the world is scary. There are links that eavesdroppers can listen in on. Information needs to be forwarded through packet switches, and these switches can be reprogrammed to listen to or modify data in transit.

  Packet switching: The path of the signal is digital, and is neither dedicated nor exclusive. A file is broken into smaller blocks, called packets. They are transmitted by following different paths and reassembled once all of them have arrived to the destination.

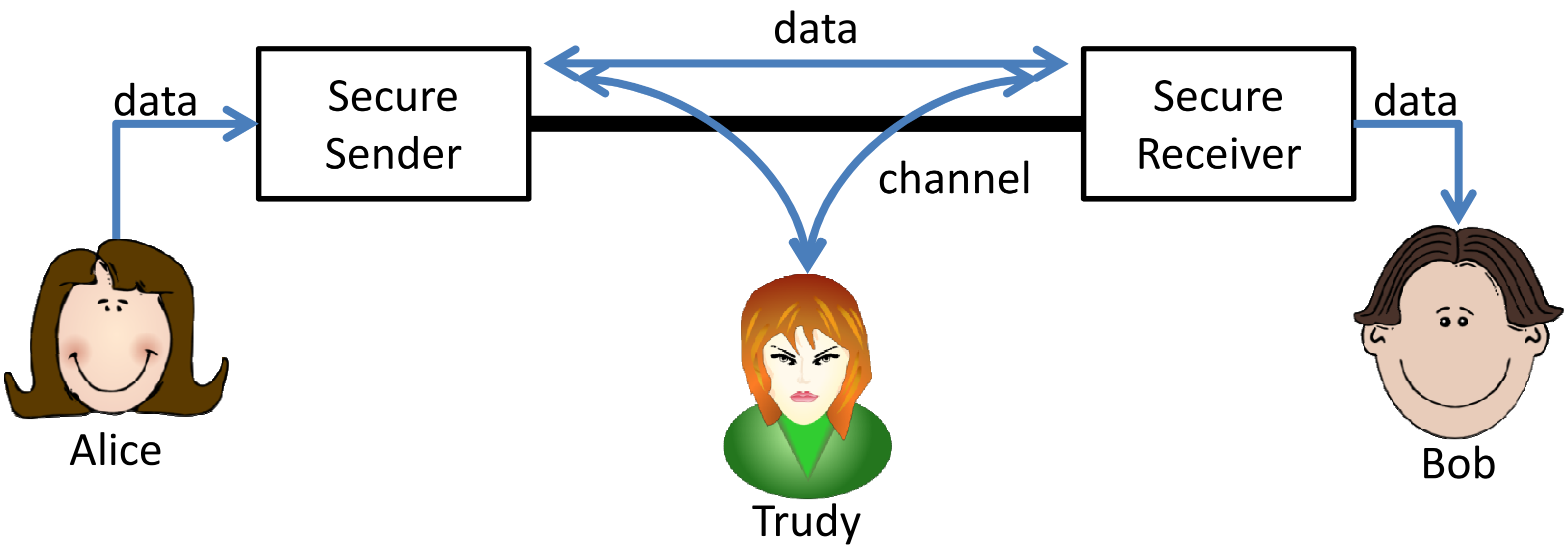
…

- **Security** and **cryptography** are different
- Informally:
  - Cryptography: keeping information secrecy
  - Security: Exploiting cryptography to deal with intruders

The basic service provided by cryptography is the ability to send information between participants in a way that prevents others from reading it. We will see also other services like authentication, integrity checking, etc.

We will concentrate on the kind of cryptography that is based on representing information as numbers and mathematically manipulating those numbers.

Alice, Bob (and Trudy)



- Alice and Bob want to communicate via a communication channel
- Trudy (the “Intruder”) wants to:
  - Intercept
  - Delete
  - Add
  - Modify

Security system’s requirements

- **Confidentiality.** Privacy or the ability to control or restrict access so that only authorized individuals can view sensitive information.
- **Integrity.** Information is accurate and reliable and has not been subtly changed or tampered with by an unauthorized party.
  - **Authenticity**: The ability to verify content.
  - **Non-repudiation & Accountability**: The origin of any action on the system can be verified and associated with a user.
- **Availability:** Information and other critical assets are accessible to customers and the business when needed.

Confidentiality

- The ability to control or restrict access so that only authorized individuals can view sensitive information.
  - Third users cannot obtain or infer information that they are not allowed to know
  - A user that is communicating cannot obtain or infer information on other communications

Integrity

- Avoid the (direct or indirect) modification of the information by user that are not allowed or due to unintentional threats

- Allow to check whether data have been modified

Authenticity

- Any user should be allowed to verify the authenticity of the information (even not confidential)

Non-repudiation & Accountability

- Each document must be associated with the user that created/modified it
  - Avoid that a user repudiates a document
  - Avoid that a user pretend to be the “owner” of a document

Availability

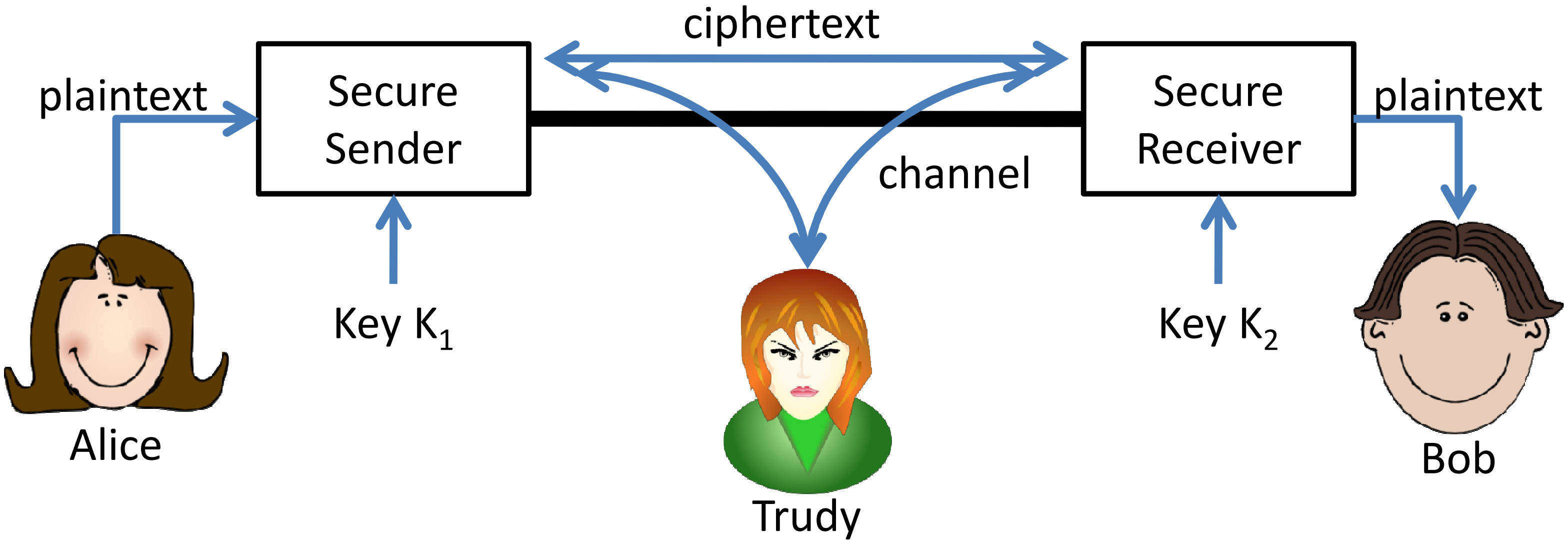
- Information is unavailable only when it is lost or destroyed, or when access to the information is denied or delayed
  - Information is available on a web site, but the server is off due to an attack.

The language of cryptography

- **Plaintext**: the original message
- **Ciphertext**: the coded message
- **Cipher**: algorithm for transforming plaintext to ciphertext
  - Encryption function or algorithm
  - Decryption function or algorithm
- **Key**: info used in cipher known only to sender/receiver

- **Cryptanalysis** (codebreaking): the study of principles/ methods of deciphering ciphertext without knowing key
- **Cryptology**: cryptography + cryptanalysis

Alice, Bob (and Trudy)



- Only Alice and Bob know the keys K_1 and K_2
- Alice, Bob, and **Trudy** know the Encryption/decryption algorithms

…

- The reason for having a key in addition to an algorithm is that it is difficult to keep devising new algorithms, and it is difficult to quickly explain a newly devised algorithm to the person with whom you'd like to start communicating securely.
- With a good cryptographic scheme it is perfectly OK to have everyone, including the bad guys (and the cryptanalysts) know the algorithm because knowledge of the algorithm without the key does not help decrypt the information.

Example

- The concept of a key is analogous to the combination for a combination lock.

- Although the concept (algorithm) of a combination lock is well known (you dial in the secret numbers in the correct sequence and the lock opens), you can't open a combination lock easily without knowing the combination.

- Notice that a bad guy can simply try all possible keys until one works. The security of a cryptographic scheme depends on how much work it is for the bad guy to break it!!!

- Keep in mind that breaking the cryptographic scheme is often only one way of getting what you want. For instance, a bolt cutter works no matter how many digits are in the combination.

… Trying all the possible keys for the combination lock example

- Let us suppose that a combination consists of three numbers, each a number between 1 and 40.
- Let us suppose it takes 10 seconds to dial in a combination.
- There are 40^3 = 64000 combinations. At 10 seconds per try, it would take a week to try all of them.
  640000/(60*60*24) ≈ 7,4 days
- What if we make the key longer?
- If the combination consists of four numbers (still from 1 to 40) then it could take 13 seconds to dial in a combination. But now with 40^4 combinations at 13 seconds per try, would take a year to try all the possibilities. (why??)

To publish or not to publish

- Some people believe that keeping a cryptographic algorithm as secret as possible will enhance its security.
- Others argue that publishing the algorithm, so that it is widely known, will enhance its security. In fact “good” guy can discover weakness and warn people.
- However if an algorithm is to be widely used it is difficult to keep the algorithm secret because it is highly likely that determined attackers will manage to learn the algorithm by reverse engineering (informally reverse engineering is an analysis in order to deduce design features from products with little or no additional knowledge about the procedures involved in their original production).
- Common practice today is for most commercial cryptosystems to be published and for military cryptosystems to be kept secret.

Definitions

- Message m: Binary string
- Encryption key: k_1 (or e)
- Decryption key: k_2 (or d)
- Encryption function or algorithm: E(m) (or $E_{k1}(m)$)
- Decryption function or algorithm: D(c) (or $D_{k2}(c)$)
- For each m:
  - E(m) = c
  - D(c) = m
  - D(E(m)) = m

Notes

- It is “computationally easy” to compute the ciphertext by using E if the key is known.
- It is “computationally easy” to compute the plaintext by using D if the key is known.
- It is “computationally hard” to compute the plaintext by using D if the key is not known.
- It is “computationally hard" to compute the keys by using E, D, m, and c.

Symmetric and Asymmetric Encryption

- Symmetric Encryption
  - Both Sender/Receiver use the same algorithms/keys for encryption/decryption
  - $K_1 = K_2$ (=K)
  - Requires sender and receiver to share a key (How? What if never met?)
- Asymmetric Encryption (Public key encryption)
  - Sender/receiver can employ different keys
  - $K_1 \neq K_2$
  - Does not require to share a key
  - K_1 (resp. K_2) can be known only to sender (resp. receiver)

Block vs. Stream ciphers

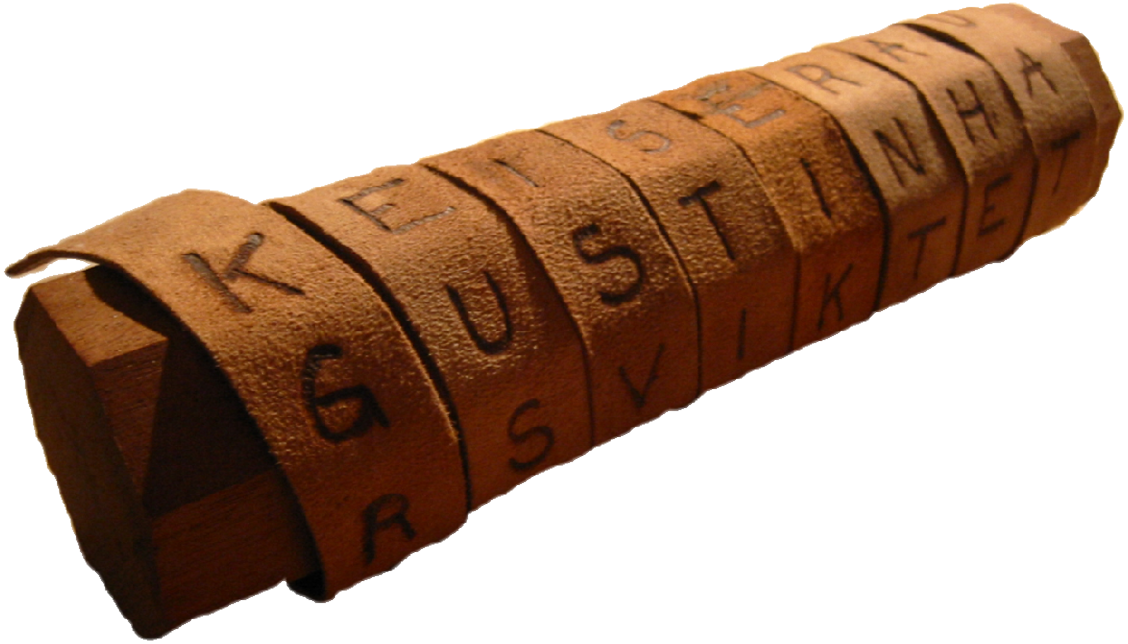
- Block ciphers encrypt block at a time
  - Message is divided into blocks and encrypted
- Stream ciphers process a bit or byte at a time during encryption/decryption

Some attackable ciphers

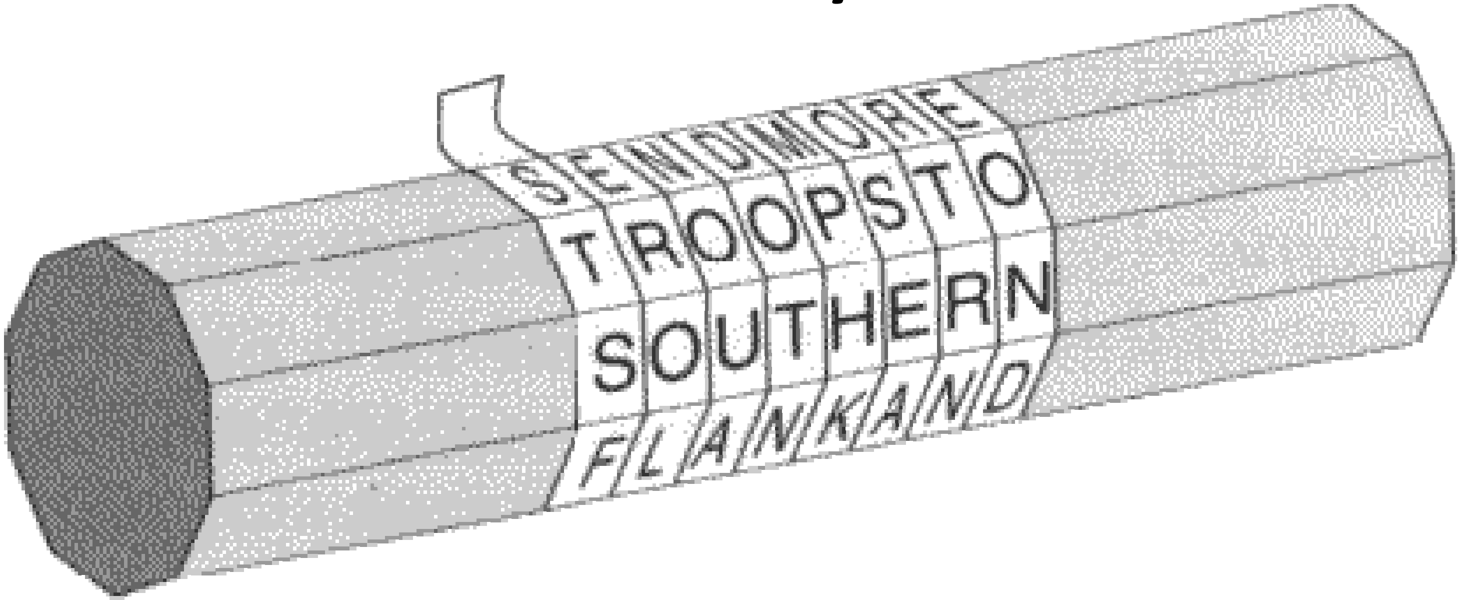
- Greek skytale (or Scytale) and transposition chipers (transposition cipher is a method of encryption by which the positions held by units of plaintext (characters or groups of characters) are shifted according to a regular system, so that the ciphertext constitutes a permutation of the plaintext.)
- Caesar cipher
- Monoalphabetic ciphers
- Polyalphabetic ciphers (Vigenère)

Greek skytale

- The ancient Greeks, and the Spartans in particular, are said to have used this cipher to communicate during military campaigns.
- It has the advantage of being fast and not prone to mistakes.
- It consists of a rod (or cylinder) with a strip of parchment (paper) wound around it on which is written a message.
- The message is written parallel to the axis.
- Then unwind the strip of parchment and send only it (without the rod)



Greek skytale



- Example:
  - PlainText: SEND MORE TROOPS TO SOUTHERN FLANK AND…..
  - Ciphertext: STSFEROLNOUADOTNMPHKOSEARTRNEOND…..

- What is the key?
  - The diameter

Indeed in order to get back to the Plaintext, the receiver has to use the same rod (or a different one but with the same diameter!)

Notice: we will often ignore punctuation marks and white spaces.

Transposition ciphers

- Greek skytale is a particular transposition cipher
- In a transposition cipher the symbols of the plaintext remain the same, but their order is changed
- Columnar Transposition Cipher
  - the plaintext is written horizontally onto a piece of graph paper of fixed width
  - The columns are chosen in some scrambled order
  - The key is the width of the paper, i.e., the number of columns, (notice that in the Skytale the diameter was the number of rows) and the permutation of the columns (in the Skytale there was no permutation).
  - Example: width = 6; Permutation: 532461
    - WE ARE DISCOVERED. FLEE IMMEDIATELY

```
  WEARED
  ISCOVE
  REDFLE
  EIMMED
  IATELY

EVLEL ACDMT ESEIA ROFME DEEDY WIREI
```

Transposition ciphers (regular)

– Consider a different plaintext:

```
WE ARE DISCOVERED. FLEE AT ONCE

      WEARED
      ISCOVE
      REDFLE
      EATONC
      EQKJEU

    EVLNE ACDTK ESEAQ ROFOJ DEECU WIREE
```

Notice we have added five meaningless characters (QKJEU) to fulfill the columns.

Decryption of transposition ciphers (1)

Suppose we have the following Ciphertext obtained by using a transposition cipher:

AESAXENTUXTVOLXEHRLXWTEFARUIQXAIYIX

How can we get back to the plaintext?

First we have to know the key!!! (what if we do not know the key? Exercise)

Suppose width=7 and permutation=3572146

Decryption of transposition ciphers (2)

AESAXENTUXTVOLXEHRLXWTEFARUIQXAIYIX

The number of characters is 35.

Since the width is 7, it means that the length of the columns is 35/7=5.

Since the permutation is 3572146, it means that the first 5 characters are of the third column, the characters from 6th to the 10th position are of the fifth column and so on.

```
WEAREAT
THEUNIV
ERSITYO
FLAQUIL
AXXXXXX
```

WE ARE AT THE UNIVERSITY OF LAQUILA XXXXXX

Decryption of transposition ciphers

Suppose we have the following Ciphertext obtained by using a transposition cipher:

AESAXENTUXTVOLXEHRLXWTEFARUIQXAIYIX

How can we get back to the plaintext, if we do not know the key?

Decryption of transposition ciphers

Given a ciphertext obtained by using a transposition cipher. How can we get back to the plaintext if we do not know the key?

Columnar transposition could be attacked by guessing all possible widths.

For each fixed width, writing the message out in its columns (but in the wrong order, as the key is not yet known), and then looking for possible anagrams.

Notice that doing anagrams help. Indeed If you do not use anagrams, for any fixed width *k*, how many possibilities do you have to try?

k! possibilities!!!

To make columnar transposition stronger, a double (irregular) columnar transposition can be used.

First let us define the irregular Columnar Transposition Cipher.

Irregular Transposition ciphers

- The columnar transposition where we added meaningless characters is called regular transposition cipher.
- In the irregular transposition cipher columns are not completed by meaningless characters.
  - Example: width = 6; Permutation: 532461

```
WE ARE DISCOVERED. FLEE AT ONCE
```

```
WEARED
ISCOVE
REDFLE
EATONC
E
```

```
EVLN ACDT ESEA ROFO DEEC WIREE
```

Double Irregular Transposition ciphers (1)

- It uses two different keys and run two times the cipher phase.
- Example: key1: width = 6; Permutation: 532461

```
 WE ARE DISCOVERED. FLEE AT ONCE


       WEARED
       ISCOVE
       REDFLE
       EATONC
       E

     EVLN ACDT ESEA ROFO DEEC WIREE
```

We now use a second key.

key2: width = 5; Permutation: 32451

Double Irregular Transposition ciphers (2)

```
EVLNACDTESEAROFODEECWIREE
```

key2: width = 5; Permutation: 32451

```
EVLNA
CDTES
EAROF
ODEEC
WIREE

LTRER VDADI NEOEE ASFCE ECEOW
```

Decryption of double irregular transposition ciphers (1)

Suppose we have the following Ciphertext obtained by using a double irregular transposition cipher:

```
LTRERVDADINEOEEASFCEECEOW
```

How can we get back to the plaintext?

First we have to know the keys!!! (if we do not know the keys, then we have to try all the possibility).

key1: width = 6; Permutation: 532461

key2: width = 5; Permutation: 32451

Decryption of double irregular transposition ciphers (2)

key1: width = 6; Permutation: 532461

key2: width = 5; Permutation: 32451

```
LTRERVDADINEOEEASFCEECEOW
```

We first decrypt by using key2:

Notice that the ciphertext has 25 characters. Since the width is 5, it means that the length of the columns is 25/5=5 for all the columns because there is no reminder.

Since the permutation is 32451, it means that the first 5 characters are of the third column, the characters from 6th to the 10th position are of the second column and so on.

```
EVLNA
CDTES
EAROF
ODEEC
WIREE

EVLNACDTESEAROFODEECWIREE
```

Decryption of double irregular transposition ciphers (3)

We now use key1: width = 6; Permutation: 532461

EVLNACDTESEAROFODEECWIREE

The ciphertext has still 25 characters. Since 25/6=4 with remainder of 1, it means that the first column contains 5 characters and all the other ones contain 4 characters.

Since the permutation is 532461, it means that the first 4 characters are of the 5th column, the characters from 5th to the 8th position are of the third column and so on.

```
WEARED
ISCOVE
REDFLE
EATONC
E
```

WE ARE DISCOVERED FLEE AT ONCE