ELECS425F
Computer and Network Security

Outline – secret-key cryptography

- One-time-pad.
- Perfect secrecy.
- Unicity distance.
- Redundancy.
  - Rates.
- Measuring and increasing security.
- Unconditional versus practical security.
- Improving security.

used only once

One-time-pad (Vernam cipher)

- Gilbert Vernam (1917/8) invented a cipher that was extended by Joseph Mauborgne to give a scheme which was later (Shannon 1949) proved to provide *perfect secrecy*.
  - We shall discuss later what *perfect secrecy* is.
- The cipher is called one-time-pad because the key is written on a long tape and is used only once.
- Encryption is by addition.
- To decrypt a cryptogram, the same key sequence must be used. Decryption is by subtracting the key sequence from the ciphertext.
- The key sequence is a truly random sequence, this was Mauborgne's contribution.

there no pattern → no repeat

[All random]

- In a one-time pad the encryption of each element of plaintext is independent of the encryption on any other piece of plaintext.
- Encryption:

  $Y_i = (X_i + K_i) \bmod 26$ Letter by letter.

  $Y_i = X_i \oplus K_i$ Bit by bit.
- Decryption:

  $X_i = (Y_i - K_i) \bmod 26$ Letter by letter.

  $X_i = Y_i \oplus K_i$ Bit by Bit

how to generate the "key tape"

very long, the same size as the plaintext

If 20 letter in plaintext

↓

key size → 20

Perfect secrecy (Shannon 1949)

- Model: Transmitter, receiver, enemy.
- Attack: *Ciphertext only*. (only get ciphertext)
- Assumption: *Enemy has unlimited power!*

  strong
- **Question 1**: Is it always possible to find the plaintext (or key)?
- **Question 2**: If it is possible, how can we measure the security?

- To find the plaintext in substitution ciphers we may use exhaustive key searches.
- For short cryptograms though, we may find multiple keys give *meaningful plaintexts*.

A	Z	N	P	T	F	Z	H	L	K	Z
m	y	s	t	e	r	y	p	l	a	y
r	e	d	b	l	u	e	c	a	k	e

- For shorter ciphertext more valid plaintext can be found.
- If the length of the ciphertext is 1, every decipherment is valid.
- For length around 50, a *unique* plaintext is likely to be found.

Perfect secrecy

- Using the knowledge of the plaintext languages a set of possible plaintexts are determined with certain probability.
- In a system with perfect secrecy, knowledge of the cryptogram does not help the enemy.

$P(X=x) = P(X=x|Y=y), \forall\ x,y$

The enemy knows Y → no help

They are just as likely to guess the plaintext associated with a ciphertext **after** they see the ciphertext as they are **before** they see it.

The enemy doesn't know Y, the cipher text

★ No key cannot decrypt although you know the cipher text

Theorem (Shannon)

In a system with perfect secrecy the number of keys is at least equal to the number of messages.

- This tells us that to achieve perfect secrecy in practice, many key bits must be exchanged. This is not practical.
- How can we measure security then if we know it probably isn't perfect?
- Shannon proposed *unicity distance* as the measure of security.

Unicity distance

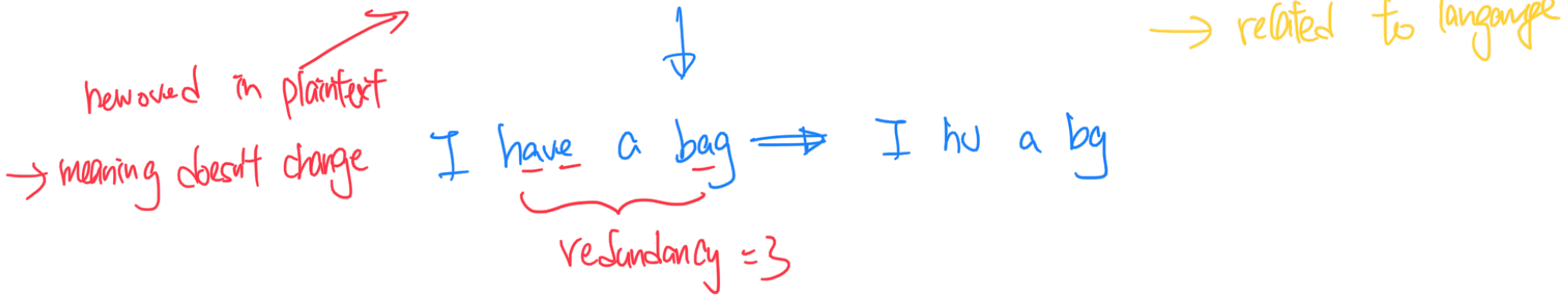
- N_0 is the least number of ciphertext characters needed to determine the key uniquely. If there are *E* keys and they are chosen with uniform probability, unicity distance is given by:

$$N_0 = \frac{\log_2 E}{d}$$

← Number of keys

← Redundancy of plaintext

where *d* is the *redundancy* of the plaintext language.



Redundancy and rates

(Information Theory)

- Redundancy of a language is defined in terms of the *rates* of the language.

  d=R-r bits

- The **absolute rate R** of a language is the maximum number of bits to represent each character, assuming characters are equally likely and emitted independently. For an alphabet of size A, $R=\log_2 A$. $= \log_2 26 (\Delta)$
- The **true rate r** of a language is the *average* number of bits required to represent characters of that language.
- For English; R ≈ 4.7 bits, r ≈ 1.5 bits, d ≈ 3.2 bits. $(d = 4.7 - 1.5)$
- True rate is always smaller than absolute rate, and the difference is the redundancy.

- All natural languages are redundant:

mst ids cn b xprsd n fwr ltrs

- This sentence is readable because we can fill all the missing characters: that is, all the missing characters are redundant.

- Redundancy is related to structure.
- A truly random source has no redundancy.

  mmhfsdacxnvfdvvdfpnfuipawedka
- Every character in this string is necessary: if one of them is omitted the information it carries is lost and cannot be recovered.

- Redundancy occurs because of the non-uniform letter frequencies, bigram (trigram …) frequencies and other (e.g. grammatical) structures of the language.

- For monoalphabetic ciphers we have:

  E=26! P(K)=1/E

  $\log_2 E \approx 88.4$ bits

  $N_0 \approx 88.4/3.2 \approx 27.6$ characters.

- Therefore cryptograms (of English text plaintext) 28 or more letters can be deciphered (in general).

Lager N_0, the more secure.

- For the one-time-pad:

  X = Message space is the set of English text of length k.

  Z = The key space which is the set of sequences of length k over the English alphabet.

  Keys are chosen randomly with uniform distribution:

  $E=26^k$, $\log_2 E \approx 4.7k$ so that

  $N_0 \approx (4.7)/(3.2)k \approx 1.47k$

  $N_0 = \frac{\log_2(X^k)}{d(K)}$

  Therefore, a *unique* solution cannot be obtained even if all the characters of the ciphertext are intercepted.

Increasing security

- Studying perfect security suggests ways of increasing security of a cipher systems.
- We could *increase the size of the key space*.
  - The increase should be such that for a ciphertext Y, using a randomly chosen key Z for decryption, a random message X should be generated.

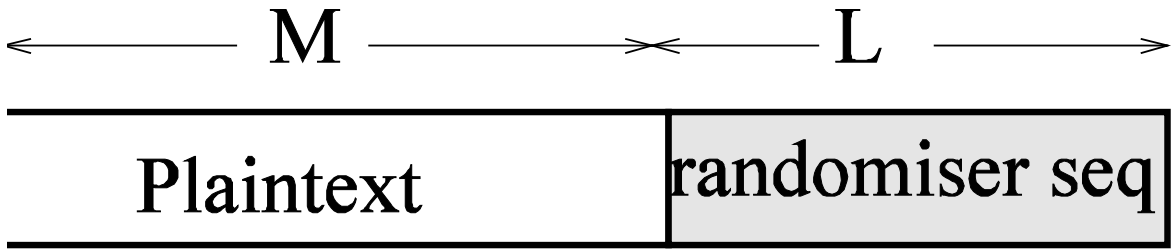
I have a bag → I hv a bg

as plaintext → less redundancy

- We could *reduce the redundancy of the plaintext language*.
  - This can be achieved using data compression.
  - A perfect data compression algorithm will result in d=0 and hence $N_0 \rightarrow \infty$, i.e. makes the cipher unbreakable.

N↑ better

- We also could use a randomiser to reduce the redundancy of the plaintext language.



$N_0 = \lim_{d \to 0} \frac{\log_2 E}{d}$

$\therefore N_0 \rightarrow \infty$

  - The new redundancy is M/(L+M)d.

Principles suggested by Shannon's work

- In the design of a good algorithm we must make methods of statistical analysis ineffective: (cannot using statical analysis)
- **Diffusion**: Diffuse the statistical structure of the plaintext into long range statistics : statistics involved long combinations of letters.
- **Confusion**: The relationship between plaintext, ciphertext and key must be complex one so that knowledge of plaintext/ciphertext pairs cannot easily be used to find the key. In other words, Y=E(X,Z) should be a *nonlinear* and complex function.

$Y = X + key$

$Y = X \cdot key$

} linear, easy to find key

$key = Y - X$

$key = \frac{Y}{X}$

Diffusion

- For example: for $X=X_1X_2\ldots$ we could use the relation

$$Y_n = E\left(\sum_{i=1}^{s} X_{n+i}\right)$$

  - This diffuses by averaging *s* consecutive letters.
  - For s=2, English alphabet, and additive cipher with shift 5 we have:

t	e	s	t	c	a	s	e
19	4	18	19	2	0	18	4
23	22	11	21	2	18	22	23
2	1	16	0	7	23	1	2
C	B	Q	A	H	X	B	C

The avalanche effect

good → DOOG
good → DAGG (X)
→ ABCD (V) cannot guess

good

- A desirable property for encryption functions is that small changes in either plaintext or key should result in significant changes in the ciphertext.
- The avalanche effect is in place if this is the case.
- For example, a cipher might be said to have the avalanche effect if a changing a single bit (in either the key or plaintext) results in half the output being different.

Confusion

- A simple additive cipher is linear.

$$Y = X \oplus Z$$

- We could use a more complex relationship. In modern ciphers the complex relationship is obtained by combining simple elements.

Block and stream ciphers

- All the substitution ciphers we have studied so far are examples of *stream ciphers*.
- In stream ciphers characters are encrypted one at a time.

- A second class of ciphers are *block ciphers.* In block ciphers plaintext characters are grouped in blocks and then each block is encrypted.
- This provides **diffusion** across the block.

Playfair cipher (1850)

- The key is specified by a 5 by 5 matrix of 25 letters.

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

Playfair cipher (1850)

- A pair of plaintext X_1X_2 is encrypted to Y_1Y_2 according to the following rules:
  - X_1X_2 in the same row: Y_1 and Y_2 are the two characters to the right of X_1 and X_2 (cyclic).
  - X_1X_2 in the same column: Y_1 and Y_2 are the two characters below X_1 and X_2 (cyclic).
  - $X_1=X_2$: A separating character (anything, X, Z …) is inserted in the plaintext between the two. This is really a pre-encryption phase.
  - X_1X_2 different rows & columns: Y_1 and Y_2 are the other two corners of the rectangle with X_1 and X_2 as corners. The direction we shall take for the example is anticlockwise from the first element to the second but this is arbitrary although we must be consistent.

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

TH	IS	IS	AT	RI	AL
PM	BH	BH	NP	HO	FS