The University of Sydney
Math3024 Elementary Cryptography and Protocols

Introduction to Cryptography

Cryptography is the study of mathematical techniques for all aspects of information security. *Cryptanalysis* is the complementary science concerned with the methods to defeat these techniques. *Cryptology* is the study of cryptography and cryptanaylsis. The security of information encompasses the following aspects:

- confidentiality or privacy,
- data integrity,
- authentication,
- nonrepudiation.

Each of these aspects of message security can addressed by standard methods in cryptography. Besides exchange of messages, tools from cryptography can be applied to sharing an access key between multiple parties so that no one person can gain access to a vault by any two of them can. Another role is in the design of electronic forms of cash.

Definitions and Terminology

Encryption = the process of disguising a message so as to hide the information it contains; this process can include both encoding and enciphering (see definitions below).

Protocol = an algorithm, defined by a sequence of steps, precisely specifying the actions of multiple parties in order to achieve an objective.

Plaintext = the message to be transmitted or stored.

Ciphertext = the disguised message.

Alphabet = a collection of symbols, also referred to as characters.

Character = an element of an alphabet.

Bit = a character 0 or 1 of the binary alphabet.

String = a finite sequence of characters in some alphabet.

Example. The following are some standard alphabets.

`A`, . . . , `Z`	26 symbols	MSDOS (less punctuation)
ASCII	7-bit words (128 symbols)	American standard
extended	8-bit words (256 symbols)	
ISO-8859-1	8-bit words (256 symbols)	European standard
Binary	{0,1}	Numerical alphabet base 2
Octal	{0,. . . ,7}	Numerical alphabet base 8
Decimal	{0,. . . ,9}	Numerical alphabet base 10
Hexadecimal	{0,. . . ,9,a,b,c,d,e,f}	Numerical alphabet base 16

Encode = to convert a message into a representation in a standard alphabet, such as to the alphabet $\{\texttt{A}, \dots, \texttt{Z}\}$ or to numerical alphabet.

Decode = to convert the encoded message back to its original alphabet and original form — the term plaintext will apply to either the original or the encoded form. The process of encoding a message is not an obscure process, and the result that we get can be considered equivalent to the plaintext message.

Cipher = a map from a space of plaintext to a space of ciphertext.

Encipher = to convert plaintext into ciphertext.

Decipher = to convert ciphertext back to plaintext.

Stream cipher = a cipher which acts on the plaintext one symbol at a time.

Block cipher = a cipher which acts on the plaintext in blocks of symbols.

Substitution cipher = a stream cipher which acts on the plaintext by making a substitution of the characters with elements of a new alphabet or by a permutation of the characters in the plaintext alphabet.

Transposition cipher = a block cipher which acts on the plaintext by permuting the positions of the characters in the plaintext.

Example. The following is an example of a substitution cipher:

$$\begin{array}{ccccccccccc}
\texttt{A} & \texttt{B} & \texttt{C} & \texttt{D} & \texttt{E} & \texttt{F} & \texttt{G} & \texttt{H} & \cdots & \texttt{Z} & \texttt{\_} \\
\downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \cdots & \downarrow & \downarrow \\
\texttt{P} & \texttt{C} & \texttt{\_} & \texttt{O} & \texttt{N} & \texttt{A} & \texttt{W} & \texttt{Y} & \cdots & \texttt{L} & \texttt{S}
\end{array}$$

which takes the plaintext `BAD CAFE BED` to the ciphertext `CPOS ANSNO`.

Cryptosystems

Given an alphabet $\mathcal{A}$ we define $\mathcal{A}^*$ to be the set of all strings over $\mathcal{A}$. In order to define a cryptosystem, we require a collection of sets:

$$\begin{array}{rlrl}
\mathcal{A} & = \text{plaintext alphabet} & \mathcal{A}' & = \text{ciphertext alphabet} \\
\mathcal{M} & = \text{plaintext space} & \mathcal{C} & = \text{ciphertext space} \\
\mathcal{K} & = \text{(plaintext) keyspace} & \mathcal{K}' & = \text{(ciphertext) keyspace}
\end{array}$$

where $\mathcal{M}$ is a subset of $\mathcal{A}^*$, $\mathcal{C}$ is a subset of $\mathcal{A}'^*$, and $\mathcal{K}$ and $\mathcal{K}'$ are sets which are generally strings of fixed finite length over some alphabets (e.g. $\mathcal{A}^n$ or $\mathcal{A}'^n$). A *cryptosystem* or *encryption scheme* is a pair (E, D) of maps

$$\begin{aligned} E &: \mathcal{K} \times \mathcal{M} \longrightarrow \mathcal{C} \\ D &: \mathcal{K}' \times \mathcal{C} \longrightarrow \mathcal{M} \end{aligned}$$

such that for each K in $\mathcal{K}$ there exists a K' in $\mathcal{K}'$ such that

$$D(K', E(K, M)) = M$$

for all M in $\mathcal{M}$. We write E_K for the map $E(K, \cdot) : \mathcal{M} \to \mathcal{C}$ and similarly write $D_{K'}$ for $D(K', \cdot) : \mathcal{C} \to \mathcal{M}$. With this notation the condition on E, D, K and K' is that $D_{K'} \circ E_K$ is the identity map on $\mathcal{M}$.

We will refer to E_K as a *cipher*, and note that a cipher is necessarily injective. For many cryptosystems, there will exist a unique inverse ciphertext key K' associated to each plaintext key K. A cryptosystem for which the inverse key K' is K itself (hence $\mathcal{K} = \mathcal{K}'$) is said to be *symmetric*. If the inverse key K' associated to K is neither K itself nor easily computable function of K, then we say that the cryptosystem is *asymmetric* or a *public key cryptosystem*.

A fundamental principle of cryptography is that the security of a cipher E_K (i.e. the difficulty in finding $D_{K'}$) does not rest on the lack of knowledge of the cryptosystem (E, D). Instead, security should be based on the secrecy of K'.

Recall that a (cryptographic) *protocol* is an algorithm, defined by a sequence of steps, precisely specifying the actions of multiple parties in order to achieve a (security) objective. An example of a cryptographic protocol, we describe the steps for message exchange using a symmetric key cryptosystem.

```
1. Alice and Bob publicly agree on a cryptosystem $(E, D)$.
2. *For each message $M$ Alice $\to$ Bob:*
   a) Alice and Bob agree on a secret key $K$.
   b) Alice computes $C = E_K(M)$ and sends it to Bob.
   c) Bob computes $M = D_K(C)$ to obtain the plaintext.
```

The difficulty of step 2.a) was one of the fundamental obstructions to cryptography before the advent of public key cryptography. Asymmetric cryptography provides an elegant solution to the problem of distribution of private keys.

Substitution Cryptosystems

Classically, cryptosystems were character-based algorithms. Cryptosystems would substitute characters, permute (or transpose) characters, or do a combination of those operations.

Notation

Throughout the course we will denote the *plaintext alphabet* by $\mathcal{A}$ and the *ciphertext alphabet* by $\mathcal{A}'$. We write E_K for the enciphering map and $D_{K'}$ for the deciphering map, where K and K' are enciphering and deciphering keys.

Substitution Ciphers

We identify four different types of substitution ciphers.

A. Simple substitution ciphers. In this cryptosystem, the algorithm is a character-by-character substitution, with the key being the list of substitutions under the ordering of the alphabet. In other words, a simple substitution cipher is defined by a map $\mathcal{A} \to \mathcal{A}'$.

Suppose that we first encode a message by purging all nonalphabetic characters (e.g. numbers, spaces, and punctuation) and changing all characters to uppercase. Then the key size, which bounds the security of the system, is 26 alphabetic characters. Therefore the total number of keys is 26!, an enormous number. Nevertheless, we will see that simple substitution is very susceptible to cryptanalytic attacks.

Example. Consider this paragraph, encoded in this way, to obtain the plaintext:

```
SUPPOSETHATWEFIRSTENCODEAMESSAGEBYPURGINGALLNONALPHABETI
CCHARACTERSEGNUMBERSSPACESANDPUNCTUATIONANDCHANGINGALLCH
ARACTERSTOUPPERCASETHENTHEKEYSIZEWHICHBOUNDSTHESECURITYO
FTHESYSTEMISALPHABETICCHARACTERSTHEREFORETHETOTALNUMBERO
FKEYSISOFENORMOUSSIZENEVERTHELESSWEWILLSEETHATSIMPLESUBS
TITUTIONISVERYSUSCEPTIBLETOCRYPTANALYTICATTACKS
```

then using the enciphering key `UVLOIDTGKXYCRHBPMZJQVWNFSAE`, we encipher the plaintext to obtain ciphertext:

```
QWMMPQDVKUVFDTXJQVDBOPIDUHDQQUGDLAMWJGXBGURRBPBURMKULDVX
OOKUJUOVDJQDGBWHLDJQQMUODQUBIMWBOVWUVXPBUBIOKUBGXBGURROK
UJUOVDJQVPWMMDJOUQDVKDBVKDCDAQXEDFKXOKLPWBIQVKDQDOWJXVAP
TVKDQAQVDHXQURMKULDVXOOKUJUOVDJQVKDJDTPJDVKDVPVURBWHLDJP
TCDAQXQPTDBPJHPWQQXEDBDNDJVKDRDQQFDFXRRQDDVKUVQXHMRDQWLQ
VXVWVXPBXQNDJAQWQODMVXLRDVPOJAMVUBURAVXOUVVUOCQ
```

Simple substitution ciphers can be easily broken because the cipher does not change the frequencies of the symbols of the plaintext.

Affine ciphers. A special case of simple substitution ciphers are the *affine ciphers.* If we numerically encode the alphabet $\{\mathtt{A}, \mathtt{B} \ldots, \mathtt{Z}\}$ as the elements $\{0, 1, \ldots, 25\}$ of $\mathbb{Z}/26\mathbb{Z}$ then we can operate on the letters by transformations of the form $x \mapsto ax + b$, for any a for which $\mathrm{GCD}(a, 26) = 1$. *What happens if a is not coprime to 26?*

An affine cipher for which $a = 1$ is called a *translation cipher*. Enciphering in a translation cipher is achieved by the performing b cyclic shift operations ($\mathtt{A} \mapsto \mathtt{B}$, $\mathtt{B} \mapsto \mathtt{C}$, etc.) on the underlying alphabet.

A classical instance of a translation cipher is the **Caesar cipher**, used by Julius Caesar, which is the translation cipher with the enciphering key $b = 3$. Using Caesar's enciphering key, we obtain the map $\mathtt{A} \mapsto \mathtt{D},\ \mathtt{B} \mapsto \mathtt{E}, \dots, \mathtt{Z} \mapsto \mathtt{C}$.

Thought Exercise. Consider the number of possible keys for the affine ciphers. Is this sufficient to have a secure cryptosystem?

B. Homophonic substitution ciphers. In this cryptosystem the deciphering is a function from a larger alphabet $\mathcal{A}'$ to the alphabet $\mathcal{A}$, but an enciphering of the plaintext can take a character to any one of the elements in the preimage.

One way to realize a homophonic cipher is to begin with m different substitution keys, and with each substitution, make a random choice of which key to use. For instance, suppose we take $\mathcal{A}$ to be own standard 26 character alphabet, and let the cipher alphabet $\mathcal{A}'$ be the set of character pairs. Suppose now that we the pair of substitution keys in the ciphertext alphabet:

```
LV MJ CW XP QO IG EZ NB YH UA DS RK TF MJ XO SL PE NU FV TC QD RK YH GW AB ZI
UD PY KG JN SH MC FT LX BQ EI VR ZA OW XP HO DJ CY RN ZV WT LA SF BM GU QK IE
```

as our homophonic key.

In order to encipher the message:

"Always look on the bright side of life."

we strip it down to our plaintext alphabet to get the plaintext string:

```
ALWAYSLOOKONTHEBRIGHTSIDEOFLIFE
```

Then each of the following strings are valid ciphertext:

```
LVRKYHLVABZVRKHOHOVRHOXPWTLXQOMJNUYHFTNBTCFVYHJNQOHOMCZABQMCSH
UDZAYHUDQKZVZAHOXODSXOMJTCLXSHMJRNBQFTNBWTZVBQXPQOHOIGZABQMCSH
LVRKYHUDQKZVRKXOXODSHOXPTCLXQOPYRNBQEZNBTCFVBQXPSHHOIGZAYHMCSH
LVZABMUDABFVRKHOHODSHOXPWTLXQOPYRNBQEZNBTCZVBQXPQOXOIGZABQMCQO
```

Moreover, each uniquely deciphers back to the original plaintext.

C. Polyalphabetic substitution ciphers. A polyalphabetic substitution cipher, like the homophonic cipher, uses multiple keys, but the choice of key is not selected randomly, rather it is determined based on the position within the plaintext. Most polyalphabetic ciphers are *periodic substitution ciphers*, which substitutes the $(mj+i)$-th plaintext character using the i-th key, where $1 \le i \le m$. The number m is called the *period*.

Vigenère cipher. The Vigenère cipher is a polyalphabetic translation cipher, that is, each of the m keys specifies an affine translation.

Suppose that we take our standard alphabet $\{\mathtt{A}, \mathtt{B}, \dots, \mathtt{Z}\}$ with the bijection with $\mathbb{Z}/26\mathbb{Z} = \{0, 1, \dots, 25\}$. Then beginning with the message:

```
Human salvation lies in the hands
 of the creatively maladjusted.
```

This gives the encoded plaintext:

```
HUMANSALVATIONLIESINTHEHANDSOFTHECREATIVELYMALADJUSTED
```

The with the enciphering key `UVLOID`, the Vigenère enciphering is given by performing the column additions:

```
HUMANS ALVATI ONLIES INTHEH ANDSOF THECRE ATIVEL YMALAD JUSTED
UVLOID UVLOID UVLOID UVLOID UVLOID UVLOID UVLOID UVLOID UVLOID
--------------------------------------------------------------
BPXOVV UGGOBL IIWWMV CIEVMK UIOGWI NCPQZH UOTJMO SHLZIG DPDHMG
```

Recall that the addition is to be carried out in $\mathbb{Z}/26\mathbb{Z}$, with the bijection defined by the following table:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

D. Polygram substitution ciphers. A polygram substitution cipher is a cryptosystem in which blocks of characters are substituted in groups. For instance (for a particular key) `AA` could map to `NO`, `AB` to `IR`, `JU` to `AQ`, etc. These cryptosystems make cryptanalysis harder by destroying the single character frequencies, preserved under simple substitution ciphers.

General affine ciphers. An affine cipher can be generalised to polygram ciphers. Rather than a map $m \mapsto c = ma + b$, we can apply a linear transformation of vectors

$$u = (m_1, \dots, m_n) \mapsto (c_1, \dots, c_n) = uA + v,$$

for some invertible matrix $A = (a_{ij})$ and vector $v = (b_1, \dots, b_n)$. As before we numerically encode an alphabet $\{\mathtt{A}, \mathtt{B} \dots, \mathtt{Z}\}$ as the elements $\{0, 1, \dots, 25\}$ of $\mathbb{Z}/26\mathbb{Z}$. Then each n-tuple of characters $m_1 m_2 \dots m_n$ is identified with the vector $u = (m_1, m_2, \dots, m_n)$. Note that matrix multiplication is defined as usual, so that

$$c_j = (\sum_{i=1}^{n} m_i a_{ij}) + b_j,$$

with the result interpretted modulo 26 as an element of $\mathbb{Z}/26\mathbb{Z}$.

As a special case, consider 2-character polygrams, so that

$$\texttt{AA} = (0,0), \dots, \texttt{ZY} = (25,24), \texttt{ZZ} = (25,25).$$

The matrix A given by

$$\begin{pmatrix} 1 & 8 \\ 21 & 3 \end{pmatrix}$$

and vector $v = (13,14)$ defines a map

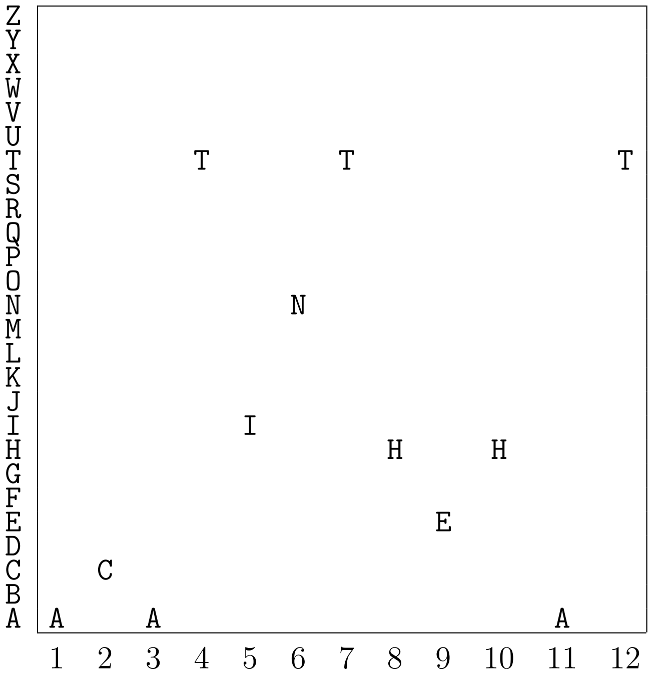
$$\begin{array}{lcl} \texttt{AA} = (\ 0,\ 0) & \mapsto & (13,14) = \texttt{NO} \\ \vdots & & \qquad\qquad\quad \vdots \\ \texttt{ZY} = (25,24) & \mapsto & (18,23) = \texttt{WA} \\ \texttt{ZZ} = (25,25) & \mapsto & (18,23) = \texttt{RD} \end{array}$$

which is a simple substitution on the 2-character polygrams. Note that the number of affine ciphers is much less than all possible substutions, but grows exponentially in the number n of characters.

Transposition ciphers.

Recall that a substitution cipher permutes the characters of the plaintext alphabet, or may, more generally, map the plaintext characters into a different ciphertext alphabet. In a *transposition cipher*, the symbols of the plaintext remain the same unchanged, but their order is permuted by a permutation of the index positions. Unlike substitution ciphers, transposition ciphers are *block ciphers*.

The relation between substitution ciphers and transposition ciphers is illustrated below. The characters and their positions of the plaintext string `ACATINTHEHAT` appear in a graph with a character axis c and a position index i for the 12 character block $1 \leq i \leq n$. We represented as a graph a substitution cipher (with equal plaintext and ciphertext alphabets) is realised as a permutation of the rows of the array, while a transposition cipher is realised by permuting the columns in fixed size blocks, in this case 12.



Permutation Groups

The symmetric group S_n is the set of all bijective maps from the set $\{1,\ldots,n\}$ to itself, and we call an elements π of S_n a permutation. We denote the n-th composition of π with itself by π^n. As a function write π on the right, so that the image of j is $(j)\pi$.

Exercise. Show that for every π in S_n, there exists an positive integer m, such that π^m is the identity map, and such that m divides $n!$. The smallest such m is called the order of π.

Notation for Permuations

The map $(j)\pi = i_j$ can be denoted by $[i_1, \dots, i_n]$. This is the way, in effect, that we have described a key for a substitution cipher — we list the sequence of characters in the image of `A`, `B`, `C`, etc. Although these permutations act on the set of the characters `A`, …, `Z` rather than the integers $1, \dots, n$, the principle is identical.

An element of S_n is called a transposition if and only if it exhanges exactly two elements, leaving all others fixed.

Exercise. How many transpositions exist in S_n? Describe the elements of order 2 in S_n. How many are there?

Exercise. Show that every element of S_n can be expressed as the composition of at most n transpositions.

Orbit Structure and Cycle Notation

Given a permutation π in S_n there exists a unique orbit decomposition:

$$\{1, \dots, n\} = \coprod_{k=1}^{t} \{(i_k)\pi^j \ : \ j \in \mathbb{Z}\},$$

where the symbol $\coprod$ refers to a disjoint union, that is, i_k is not equal to $(i_\ell)\pi^j$ for any j unless $k = \ell$. The sets $\{(i_k)\pi^j \ : \ j \in \mathbb{Z}\}$ are called the *orbits* of π, and the cycle lengths of π are the sizes $d_1, \dots, d_t$ of the orbits.

Asociated to any orbit decomposition we can express an element π as

$$\pi = \big(i_1, (i_1)\pi, \dots, (i_1)\pi^{d_1-1}\big) \cdots \big(i_t, (i_t)\pi, \dots, (i_t)\pi^{d_t-1}\big)$$

Note that if $d_k = 1$, then we omit this term, and the identity permutation can be written just as 1. This notation gives more information about the permutation π and is more compact for simple permutations such as transpositions.

Exercise. What is the order of a permuation with cycle lengths $d_1, \dots, d_t$? How does this solve the previous exercise concerning the order of a permuation?

Simple Columnar Transposition

The simplest example of a transposition cipher is an (r, s)-simple columnar transposition. In this cryptosystem the plaintext is written in blocks as r rows of fixed length s. The ciphertext is read off as the columns of this array. Suppose we begin with the plaintext:

```
I was riding on the Mayflower
When I thought I spied some land
I yelled for Captain Arab
I have yuh understand
Who came running to the deck
Said, "Boys, forget the whale
Look on over yonder
Cut the engines
Change the sail
Haul on the bowline"
We sang that melody
Like all tough sailors do
When they are far away at sea
```

Stripped to our plaintext alphbet and written in lines of 36 characters each, we have the plaintext:

```
IWASRIDINGONTHEMAYFLOWERWHENITHOUGHT
ISPIEDSOMELANDIYELLEDFORCAPTAINARABI
HAVEYUHUNDERSTANDWHOCAMERUNNINGTOTHE
DECKSAIDBOYSFORGETTHEWHALELOOKONOVER
YONDERCUTTHEENGINESCHANGETHESAILHAUL
ONTHEBOWLINEWESANGTHATMELODYLIKEALLT
OUGHSAILORSDOWHENTHEYAREFARAWAYATSEA
```

Reading off the columns, we obtain the following ciphertext under the columnar transposition cipher:

```
IIHDYOOWSAEONUAPVCNTGSIEKDHHREYSEESIDUARBADSHICOIIOUDUWL
NMNBTLOGEDOTIROLEYHNSNARSEEDTNSFEWOHDTONEWEIARGSHMYNGIAE
AEDENNNYLWTEGTFLHTSTHLEOHCHEODCEHAYWFAWATAEOMHNMRRREAGEE
WCRLELFHAUETOAEPNLHDRNTNOEYAIAIOSLWTINKAIAHNGOIKYOATNLEA
UROOHATGATVALSHBHEULETIERLTA
```

Exercise. What is the block length m of an (r, s)-simple columnar transposition? Describe the permutation. Hint: it may be easier to describe the permutation if the index set is $\{0, \ldots, m-1\}$.

Exercise. Show that the (r, r)-simple columnar transposition has order 2. What is the order of the cipher for $(r, s) = (3, 5)$? What are the cycle lengths?

Cryptanalysis of Transposition Ciphers

A transposition cipher can easily be recognized by an analysis of character frequencies. Iterating transposition ciphers can greatly increase security, but as with substitution ciphers, almost all such ciphers can be broken. Although many modern cryptosystems incorporate transposition ciphers, the operation on large blocks has the disadvantage of requiring a lot of memory.

Enigma and Rotor Machines

Background on rotor machines and, in particular, the Enigma, will be covered in the lectures only.