Lecture 3

Classical Cryptography

UTAS
Sultanate of Oman
September 2022

CSSY2201 : Introduction to Cryptography

جامعة التقنية
والعلوم التطبيقية
University of Technology
and Applied Sciences
Salalah صلالة

Plan

Plan

Cesar

- Consists of replacing letters in the plaintext with other letters or symbols or bits.
- the best known is Cesar's alg : replace each letter by the one that follows it after three positions in the alphabet
- The alphabet is wrapped so that the letter following Z is A
- ex :

plaintext :	meet	me	after	the	toga	party
ciphertext :	phhw	ph	diwhu	wkh	wrjd	sduwb

Cesar

- We can describe Cesar by this following substitution :

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
d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c

- Cesar Encryption can be expressed by :

$$c = E(3, p) = (p + 3) mod\, 26$$

- The shifting can be generalised to any number k :

$$c = E(k, p) = (p + k) mod\, 26$$

- if $k \in [1, 25]$, then Cesar decryption is expressed by :

$$p = D(k, c) = (c - k) mod\, 26$$

- where $p = 0, 1, 2, \ldots, 25$ corresponding to the alphabet letters $a, b, \ldots, z$
- ex :

$$E(3, "a") = (0 + 3) mod\, 26 = 3 = "d"$$

$$E(3, "b") = (1 + 3) mod\, 26 = 4 = "e"$$

$$E(3, "m") = (12 + 3) mod\, 26 = 15 = "p"$$

$$E(3, "x") = (23 + 3) mod\, 26 = 0 = "a"$$

$$E(3, "y") = (24 + 3) mod\, 26 = 1 = "b"$$

$$E(3, "z") = (25 + 3) mod\, 26 = 2 = "c"$$

Brute force attack on Cesar :try all 26 combinations

KEY	PHHW PH DIWHU WKH WRJD SDUWB
1	oggv og chvgt vjg vqic rctva
2	nffu nf bgufs uif uphb qbsuz
3	meet me after the toga party
4	ldds ld zesdq sgd snfz ozqsx
5	kccr kc ydrcp rfc rmey nyprw
6	jbbq jb xcqbo qeb qldx mxoqv
7	iaap ia wbpan pda pkcw lwnpu
8	hzzo hz vaozm ocz ojbv kvmot
9	gyyn gy uznyl nby niau julns
10	fxxm fx tymxk max mhzt itkmr
11	ewwl ew sxlwj lzw lgys hsjlq
12	dvvk dv rwkvi kyv kfxr grikp
13	cuuj cu qvjuh jxu jewq fqhjo
14	btti bt puitq iwt idvp epqin
15	assh as othsf hvs hcuo dofhm
16	zrrg zr nsgre gur gbtn cnegl
17	yqqf yq mrfqd ftq fasm bmdfk
18	xppe xp lqepc esp ezrl alcej
19	wood wo kpdob dro dyqk zkbdi
20	vnnc vn jocna cqn cxpj yjach
21	ummb um inbmz bpm bwoi xizbg
22	tlla tl hmaly aol avnh whyaf
23	skkz sk glzkx znk zumg vgxze
24	rjjy rj fkyjw ymj ytlf ufwyd

Plan

Monoalphabetic Cipher

- consists of replacing each letter arbitrarily (not a simple shift)
- the key is of length 26 :

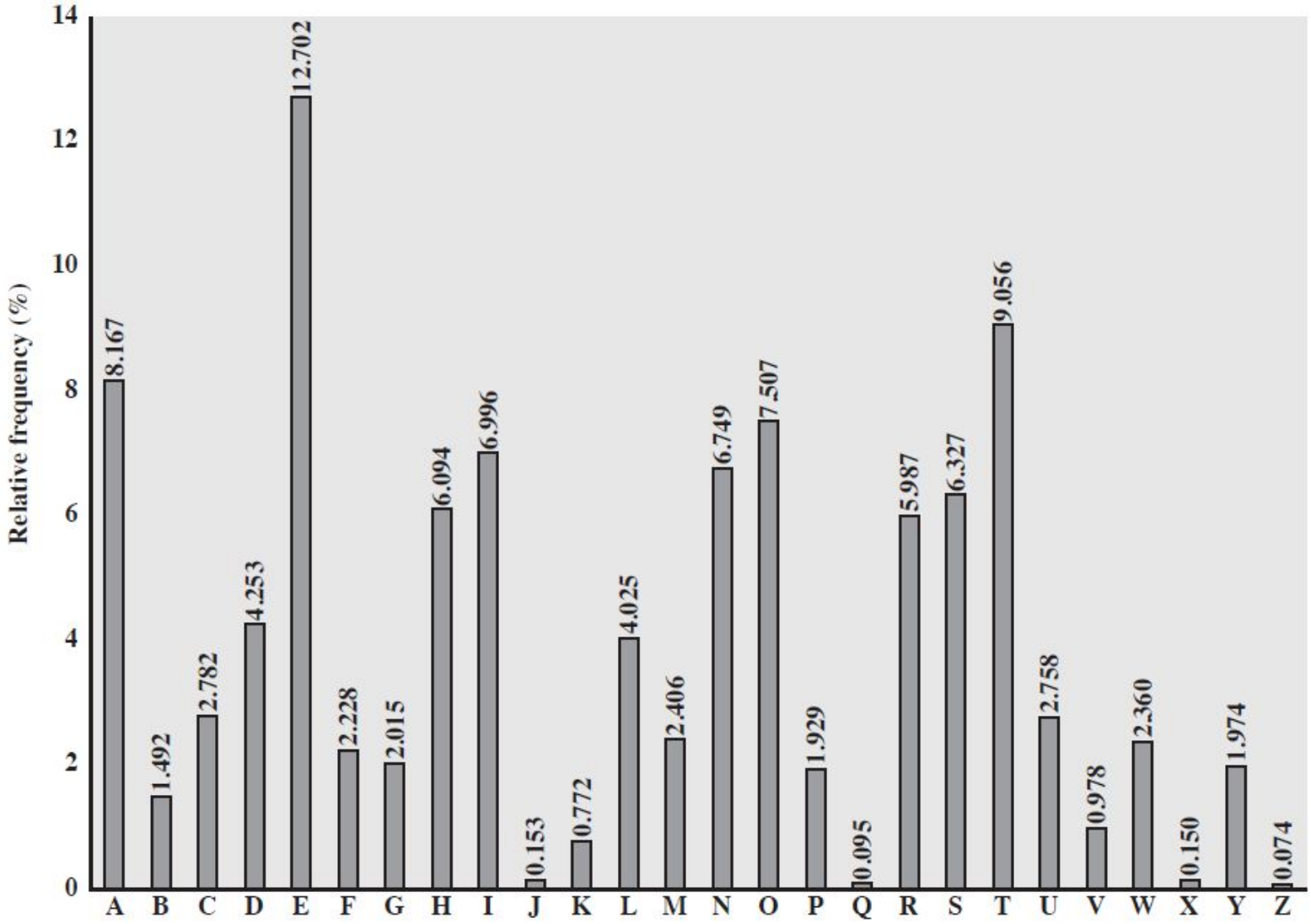
a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
d	k	v	q	f	i	b	j	w	p	e	s	c	x	h	t	m	y	a	u	o	l	r	g	z	n

- example :
  Plaintext : if we wish to replace letters
  Ciphertext : wi rf rwaj uh yftsdvf sfuufya

Security of monoalphabetic cipher

- We have a total of $26! = 4 \times 10^{26}$ possible keys
- but it can be broken by frequency analysis : Al-Kindy
- human language is very redundant
- ex : in the msg "th lrd s m shphrd shll nt wnt" letters like this are not ordinary in English
- In English the letter "E" is the most used, followed by : "T,R,N,I,O,A,S"
- letters like "Z,J,K,Q,X" are rare in use.
- there are doubles or triples that are answered more than others.

letters frequencies in english



Example of a Cryptanalysis using frequencies

- given a ciphertext :
  UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXU
  DBMETSXAIZVUEPHZHMDZSHZOWSFPAPPDTSV
  PQUZWYMXUZUHSXEPYEPOPDZSZUFPOMBZWPF UPZHMDJUDTMOHMQ
- We count the frequency of each letter in the ciphertext
- We can guess that P and Z are e and t
- We can guess that ZW is th and therefore ZWP is the
- the sequence ZWSZ is replaced by th*t, we can guess that S is a

```
UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
 t a        e  e te  a that e e a        a
VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
   e t   ta t ha e ee   a e  th    t  a
EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ
 e  e e tat  e   the   t
```

- we continue with the trial-error-trial technique, we find the plaintext :
  "it was disclosed yesterday that several informal but direct contacts have been made with political representatives of the viet cong in moscow"

Plan

Playfair

- The best known alg that encrypts several letters at the same time
- treats diagrams (2 letters) as a unit and converts it to a ciphertext diagram.
- based on matrix 5×5 using keyword
- invented by the British Sir Charles Wheatstone in 1854
- used by the British army in W.W.I and by the USA and its allies during the W.W.II war

Playfair Matrix

- copy the letters of the keyword in the matrix (without duplication)
- complete the rest of the matrix with the missing letters
- the letters I and J are treated as a single letter
- ex : using the keyword MONARCHY

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

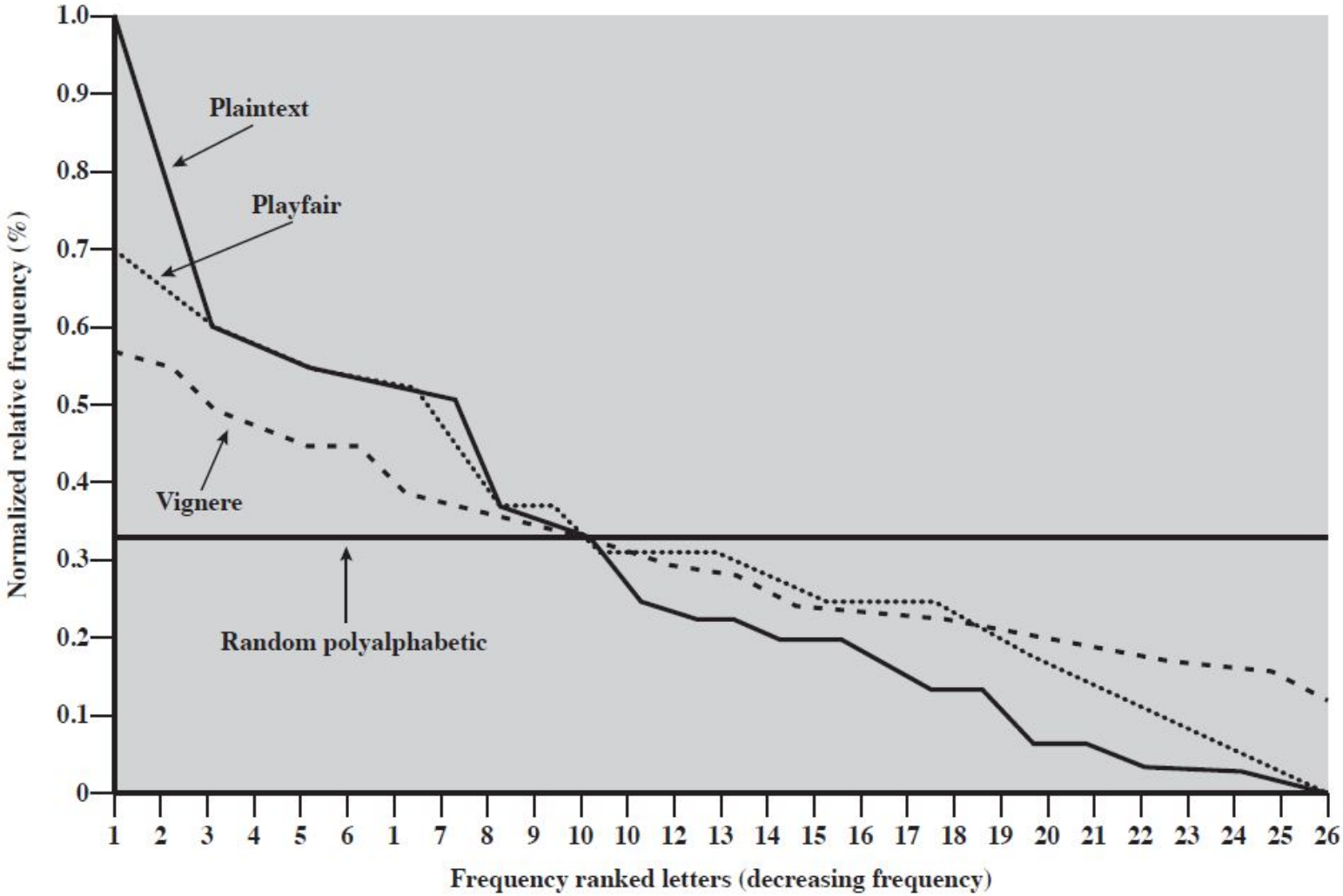
Playfair Encryption

- operate on letter diagrams (2 letters) each time
- particular case : if diagram of the same letters, separate by special letters ex : x. for example : balloon is treated as ba lx lo on
- If plaintext in the same line : replace with the letters on the right. Ex1 pq is replaced by qs. Ex2 ar is replaced by RM.
- If plaintext in the same column : replace with the letters below. ex mu is replaced by CM
- otherwise, replace by letter in the same line as it and same column as the other letter of the plaintext. ex1 : hs is replaced by BP. ex2 : ea becomes IM or JM

Security of Playfair

- Improved security since there are a total of $26 \times 26 = 676$ diagrams
- we need a frequency analysis on 676 units and no longer on 26 like the monoalphabetic
- so the ciphertext alphabet is also huge
- but it can be broken if we know a hundred of plaintext/ciphertext...

letter frequency



Plan

Polyalphabetic Ciphers

- poly-alphabetic substitution algorithm
- improves security by combining several mono-alphabetic algs
- makes cryptanalysis more difficult with increased alphabets and a flatter frequency distribution
- uses a key to choose which mono-alphabetic alphabet to use for each letter in the plaintext
- repeat from beginning if end of key is reached

Vigenere

- the simplest polyalphabetic alg : multiple Cesar algs
- the key consists of characters $K = k_1 k_2 \ldots k_d$
- the ith letter of the key specifies the ith Cesar alg to use
- repeat from the beginning each d letters of the plaintext

		Plaintext																							
		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
Key	a	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
	b	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
	c	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
	d	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
	e	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
	f	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
	g	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
	h	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
	i	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
	j	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
	k	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
	l	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
	m	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
	n	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
	o	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
	p	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
	q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
	r	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
	s	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
	t	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
	u	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
	v	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
	w	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U

Example VigenÃ¨re

- write the plaintext
- write the key and repeat it over the length of the plaintext
- use each letter of the key as Cesar's key
- encrypt each letter independently of the others
- eg : key=deceptive

```
key:            deceptivedeceptivedeceptive
plaintext:      wearediscoveredsaveyourself
ciphertext:     ZICVTWQNGRZGVTWAVZHCQYGLMGJ
```

Autokey cipher

- wanting a key as long as the message
- vigenere offers the autokey
- key is prefixed to the message to generate a new key
- knowing the basic key, we can decipher the first letters
- can be broken by frequency analysis...
- ex : key :deceptive

```
key:          deceptivewearediscoveredsav
plaintext:    wearediscoveredsaveyourself
ciphertext:   ZICVTWQNGKZEIIGASXSTSLVVWLA
```

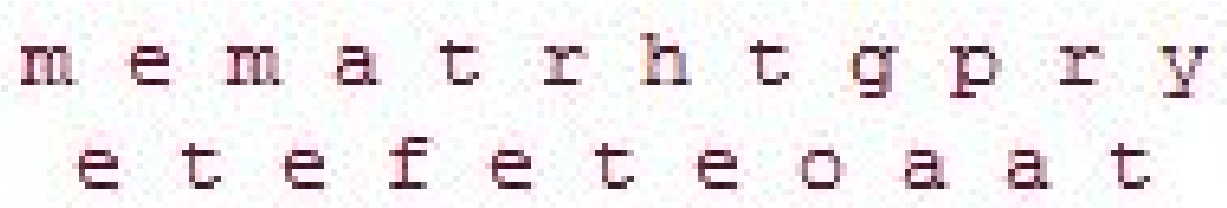
Plan

Transposition

- Transposition= permutation
- Encrypt the message by rearranging the order of the plaintext letters
- plaintext and ciphertext have same occurrence (frequency) of letters

Fail hence cipher

- The simplest transposition
- plaintext is written in sequences of diagonals
- we read it line by line
- to encrypt the message "meet me after the toga party" with "Rail hence" of depth (nb of lines) 2 :



- ciphertext is : MEMATRHTGPRYETEFETEOAAT

Raw Transposition Cipher

- More complex transposition
- write the plaintext as a rectangle, line by line
- ciphertext : read the message column by column, but swap the order of the columns
- "the order of reading the columns" is the key

```
Key:          4 3 1 2 5 6 7
Plaintext:    a t t a c k p
              o s t p o n e
              d u n t i l t
              w o a m x y z
Ciphertext:   TTNAAPTMTSUOAODWCOIXKNLYPETZ
```

Product ciphers

- Substitution or transposition algorithms are not secure because of frequency analysis
- therefore consider using several algs in a row to make cryptanalysis more difficult.
- example repeat the permutation of the previous text with the same key (or even with another key) :

```
Key:        4 3 1 2 5 6 7
Input:      t t n a a p t
            m t s u o a o
            d w c o i x k
            n l y p e t z
Output:     NSCYAUOPTTWLTMDNAOIEPAXTTOKZ
```

Product ciphers

- we can see the effect of the double permutation like this :
  - before swapping :

```
01 02 03 04 05 06 07 08 09 10 11 12 13 14
15 16 17 18 19 20 21 22 23 24 25 26 27 28
```

  - after the first permutation :

```
03 10 17 24 04 11 18 25 02 09 16 23 01 08
15 22 05 12 19 26 06 13 20 27 07 14 21 28
```

  - after the second permutation :

```
17 09 05 27 24 16 12 07 10 02 22 20 03 25
15 13 04 23 19 14 11 01 26 21 18 08 06 28
```

- This is the concept of modern encryption algorithms
- Standards like DES, 3-DES and AES are prodcuts ciphers.