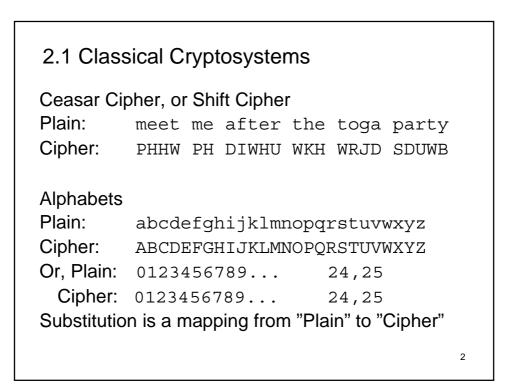
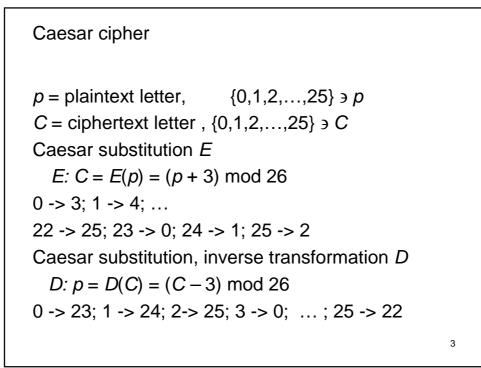
T-79.159 Cryptography and Data Security

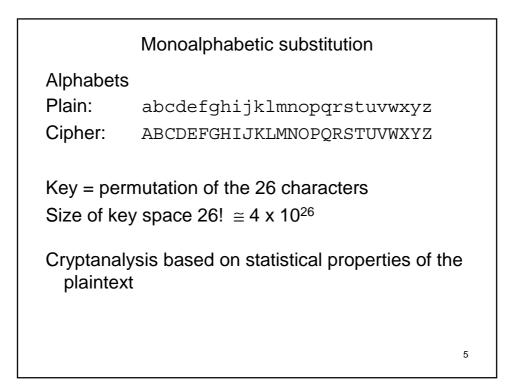
Lecture 2:

2.1 Classical cryptosystems2.2.Introduction to modern cryptographic primitivesKaufman et al: Chapter 2Stallings: Chapter 2





```
Brute force cryptanalysis of shift cipher
Shift cipher: E: C = E(p) = p + K mod 26
K = key; {0,1,2,3,...,25} > K
We need only some piece of ciphertxt to do exhaustive search
K PHHW PH DIWHU WKH WRJD SDUWB
1 oggv ...
2 nffu ...
3 meet me after the toga party
```



	- 1	of Letters i	<u>_</u>	
		N	6.749	
A	8.167			
В	1.492	0	7.507	
С	2.782	Р	1.929	
D	4.253	Q	0.095	
E	12.702	R	5.987	
F	2.228	S	6.327	
G	2.015	Т	9.056	
н	6.094	U	2.758	
1	6.996	V	0.978	
J	0.153	W	2.360	
к	0.772	х	0.150	
L	4.025	Y	1.974	
М	2.406	Z	0.074	

```
<section-header><section-header>
```

	Frequ	ency ta	adie	
	.			
А	0	Ν	9	
В	1	0	0	
С	15	Р	1	
D	13	Q	4	
E	7	R	10	
F	11	S	3	
G	1	Т	2	
н	4	U	5	
1	5	V	5	
J	11	W	8	
К	1	Х	6	
L	0	Y	10	
М	16	Z	20	

```
Simple substitution: frequency analysis cont'd

The most frequent character: Z

The most frequent character in English: e

Guess: D(Z) = e

The next most frequent characters

{M, C, D, F, J, R, Y, N}

The next most frequent characters in English

{t, a, o, i, n, s, h, r}

The most frequent digrams with Z are:

DZ, ZW (4 times); NZ, ZU (3 times);

RZ, HZ, XZ, FZ, ZR, ZV, ZC, ZD (two times each)
```

```
Using comon digrams...

NZ is common but ZN occurs only once;

guess D(N) = h

ZW is common and WZ not at all and W is rare;

guess D(W) = d

DZ (4 times) and ZD (2 times) are both common

we guess \{r, s, t\} \neq D(D)

ZRW and RZW occur, and RW occurs, and R is

frequent we guess D(R) = n
```

Now	we ha	ve					
	end		е	ne	dh e		
YIFQF	MZRWQ	FYVEC	FMDZP	CVMRZ	WNMDZ	VEJBT	
	h		е	е		nh d	
XCDDU	MJNDI	FEFMD	ZCDMQ	ZKCEY	FCJMY	RNCWJ	
en	е	h eh	n		n	ed	
CSZRE	XCHZU	NMXZN	ZUCDR	JXYYS	MRTME	YIFZW	
е	е	ne nd	he e	ed	n	h h	
DYVZV	YFZUM	RZCRW	NZDZJ	JXZWG	CHSMR	NMDHN	
	е	ed		d he	n		
CMFQC	HZJMX	JZWIE	JYUCF	WDJNZ	DIR		
ne_ndhe suggests that <i>D</i> (C) = a							

end a e a ne dh e YIFQF MZRWQ FYVEC FMDZP CVMRZ WNMDZ VEJBT h ea nhad а ea а XCDDU MJNDI FEFMD ZCDMQ ZKCEY FCJMY RNCWJ a en a e h eh a n n ed CSZRE XCHZU NMXZN ZUCDR JXYYS MRTME YIFZW neand he e е ed a n h h е DYVZV YFZUM RZCRW NZDZJ JXZWG CHSMR NMDHN ed a a e a d he n CMFQC HZJMX JZWIE JYUCF WDJNZ DIR nh decrypts to RNM suggests that D(M) = i or o12

```
We have
      iend
                 a i e a ine dhi e
YIFQF MZRWQ FYVEC FMDZP CVMRZ WNMDZ VEJBT
      i h
                i
                   ea i
                                 a i
 а
                           ea
                                       nhad
XCDDU MJNDI FEFMD ZCDMQ ZKCEY FCJMY RNCWJ
       a e
            hi eh
                     a n
                                in i
a en
                                          ed
CSZRE XCHZU NMXZN ZUCDR JXYYS MRTME YIFZW
        e i neand he e
                            ed
                                а
                                    in hi
                                           h
   е
DYVZV YFZUM RZCRW NZDZJ JXZWG CHSMR NMDHN
   а
       еi
              ed
                          d he
ai
                       а
                                  n
CMFQC HZJMX JZWIE JYUCF WDJNZ DIR
Guess \{D, F, J, Y\} \rightarrow E(o), then Y is the most likely
                                               13
```

```
iend
             o a
                   i e a ine dhi e
0
YIFQF MZRWQ FYVEC FMDZP CVMRZ WNMDZ VEJBT
               i
      i h
                  ea i
                         ea o
                                a io nhad
 а
XCDDU MJNDI FEFMD ZCDMQ ZKCEY FCJMY RNCWJ
       ae hiehean
a en
                          00
                               in i
                                     0
                                        ed
CSZRE XCHZU NMXZN ZUCDR JXYYS MRTME YIFZW
 o e o e i neand he e
                                  in hi
                          ed
                              а
                                         h
DYVZV YFZUM RZCRW NZDZJ JXZWG CHSMR NMDHN
       еi
             ed
                        d he
ai a
                   оa
                                 n
CMFQC HZJMX JZWIE JYUCF WDJNZ DIR
Remaining {D, F, J} possibly decrypt to {r, s, t}
                                            14
```

Remaining {D, F, J} possibly decrypt to {r, s, t}										
orriend	ro a	rise	a ine	dhise	t					
YIFQF MZRWQ	FYVEC	FMDZP	CVMRZ	WNMDZ	VEJBT					
ass iths	r ris	easi	ea	rati	nhadt					
XCDDU MJNDI	FEFMD	ZCDMQ	ZKCEY	FCJMY	RNCWJ					
a en a e	hi eh	asn	t oo	in i	o red					
CSZRE XCHZU	NMXZN	ZUCDR	JXYYS	MRTME	YIFZW					
so e re i	neand	heset	ed	a in	his h					
DYVZV YFZUM	RZCRW	NZDZJ	JXZWG	CHSMR	NMDHN					
air a eti	ted	to ar	dsthe	s n						
CMFQC HZJMX	JZWIE	JYUCF	WDJNZ	DIR						

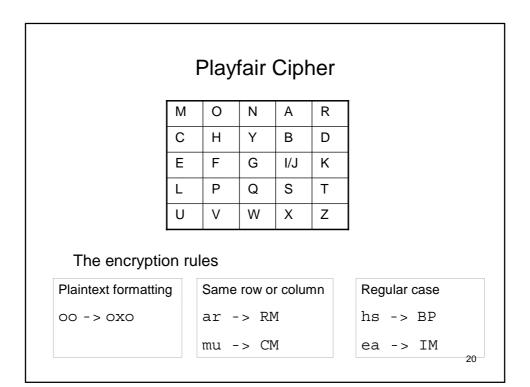
Try D(g) = f and so on ..

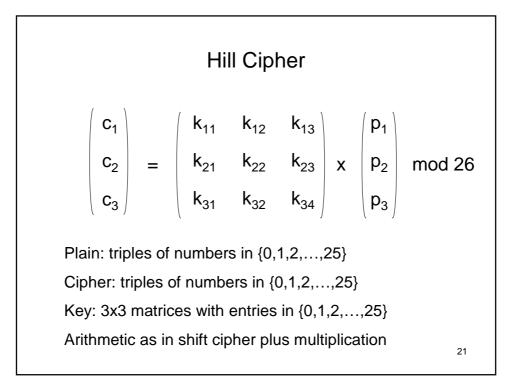
ourfriendfrorisea inedhisetYIFQFMZRWQFYVECFMDZPCVMRZWNMDZVEJBTassithsur riseasifea orationhadtXCDDUMJNDIFEFMDZCDMQZKCEYFCJMYRNCWJa ena ehi ehe asnt ooin iouredCSZREXCHZUNMXZNZUCDRJXYYSMRTMEYIFZWso eore ineandhesett eda inhis hDYVZVYFZUMRZCRWNZDZJJXZWGCHSMRNMDHNairfaetiteduto ardsthesunCMFQCHZJMXJZWIEJYUCFWDJNZDIR

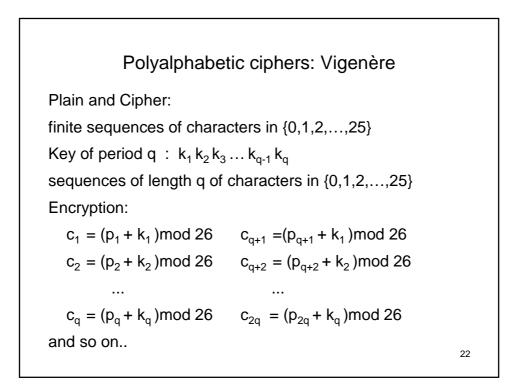
17

ourfr iendf rom a rise amine dhise m t YIFQF MZRWQ FYVEC FMDZP CVMRZ WNMDZ VEJBT ass ithsu r ris easif ea o ratio nhadt XCDDU MJNDI FEFMD ZCDMQ ZKCEY FCJMY RNCWJ a en a e hi eh e asn t oo in i oured CSZRE XCHZU NMXZN ZUCDR JXYYS MRTME YIFZW somem ore i neand heset t ed a in his h DYVZV YFZUM RZCRW NZDZJ JXZWG CHSMR NMDHN airfa eti tedu to ar dsthe sun CMFQC HZJMX JZWIE JYUCF WDJNZ DIR

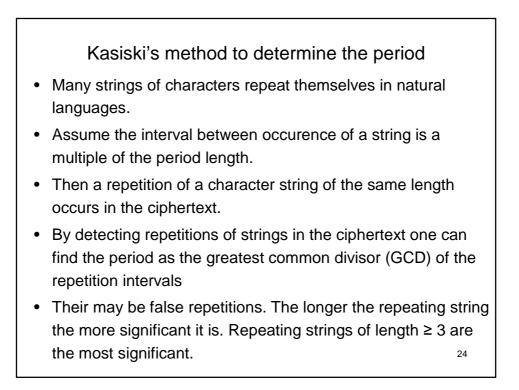
ourfr	iendf	rompa	risex	amine	dhise	mptyg	
YIFQF	MZRWQ	FYVEC	FMDZP	CVMRZ	WNMDZ	VEJBT	
lassw	ithsu	rpris	easif	evapo	ratio	nhadt	
XCDDU	MJNDI	FEFMD	ZCDMQ	ZKCEY	FCJMY	RNCWJ	
akenp	lacew	hileh	ewasn	tlook	ingip	oured	
CSZRE	XCHZU	NMXZN	ZUCDR	JXYYS	MRTME	YIFZW	
somem	orewi	neand	heset	tledb	ackin	hisch	
DYVZV	YFZUM	RZCRW	NZDZJ	JXZWG	CHSMR	NMDHN	
airfa	cetil	tedup	towar	dsthe	sun		
CMFQC	HZJMX	JZWIE	JYUCF	WDJNZ	DIR		
							19

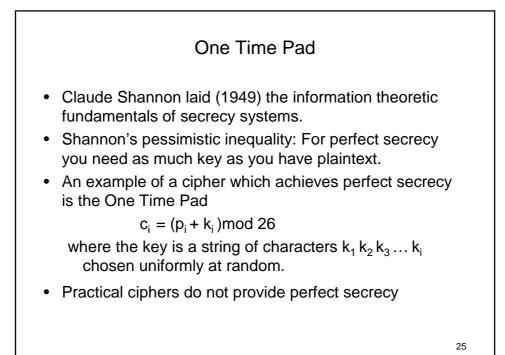


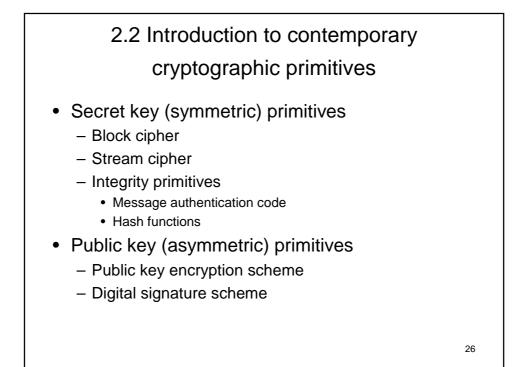


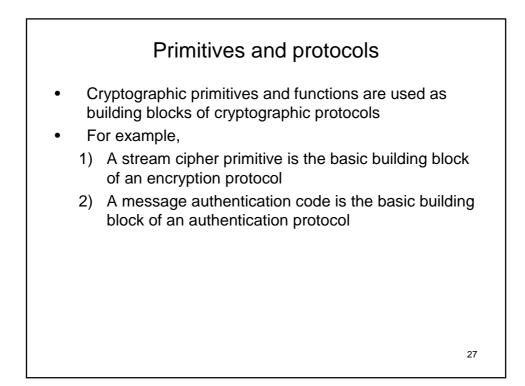


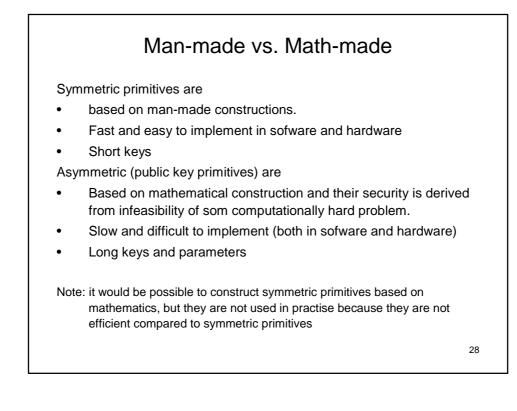
```
Polyalphabetic ciphers: VigenèreExampleourfr iendf rompa risex amine dhise mptyg<br/>מַרוֹם מַרָּשַׁר וַמַפַּר ווּמַפַּר ווּמַפַּר ווּמַפּר ווּמַפּרJINE OWCUN בעיר בייStote the repetition of a two character string resulting from a<br/>ceptition in the plaintext:
```

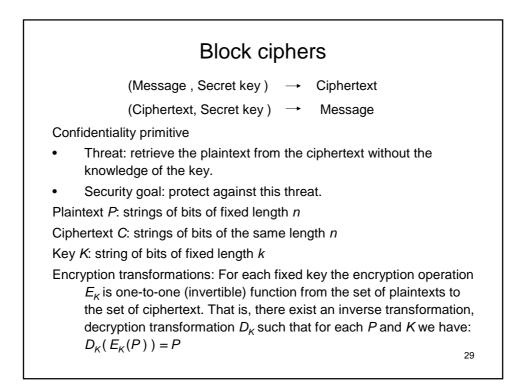


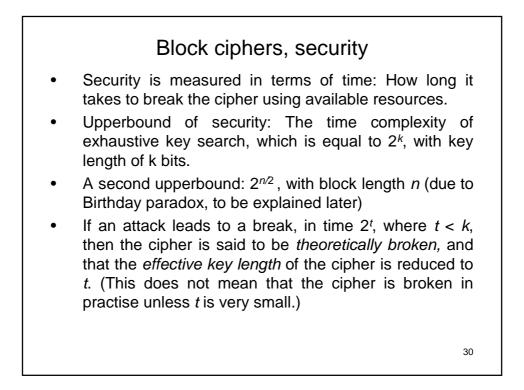






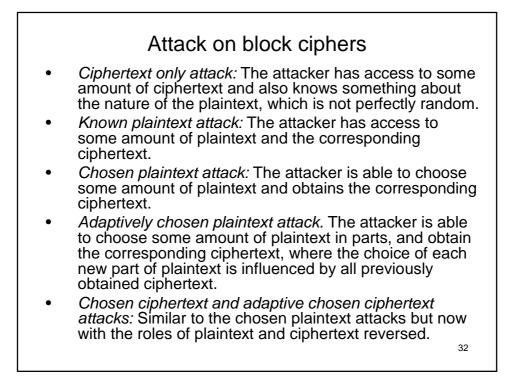


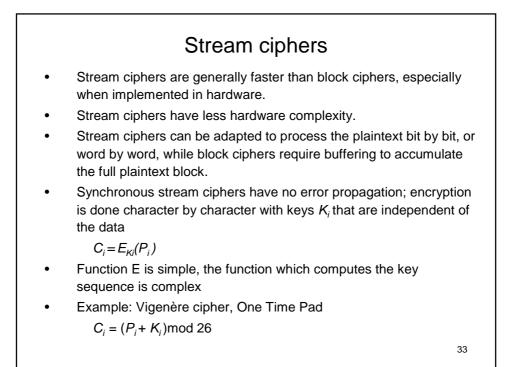


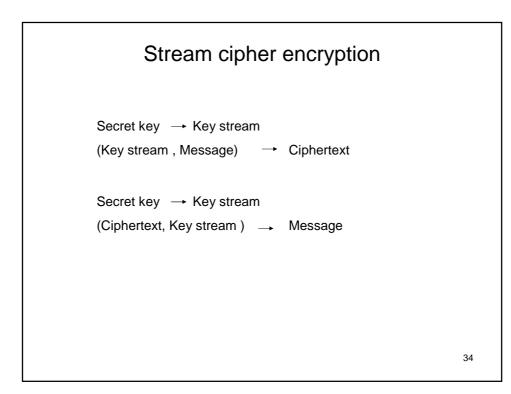


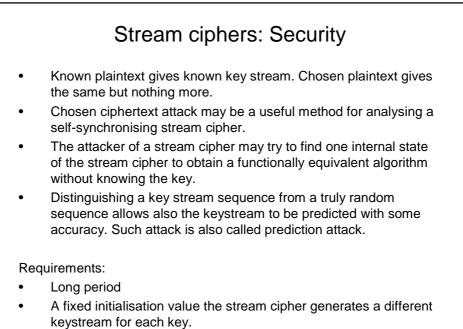
Block ciphers, design principles

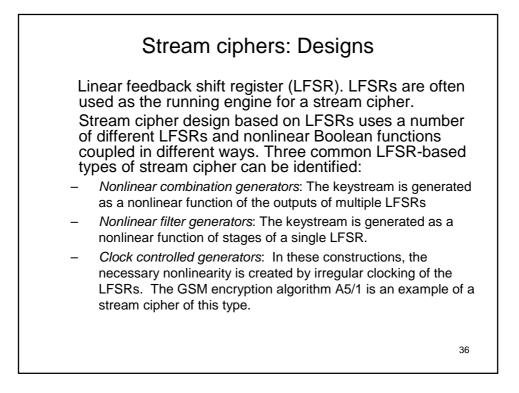
- The ultimate design goal of a block cipher is to use the secret key as efficiently as possible.
- Confusion and diffusion (Shannon)
- New design criteria are being discovered as response to new attacks.
- A state-of-the-art block cipher is constructed taking into account all known attacks and design principles.
- But no such block cipher can become provably secure, it may remain open to some new, unforeseen attacks.
- Common constructions with iterated round function
 - Substitution permutation network (SPN)
 - Feistel network

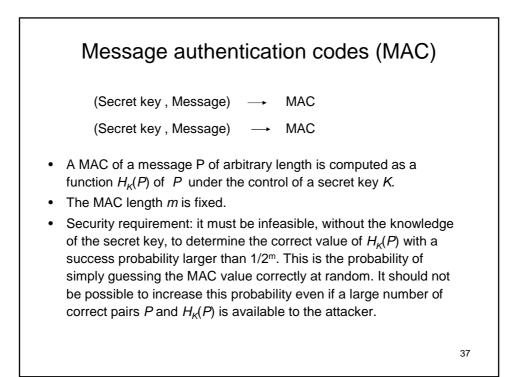


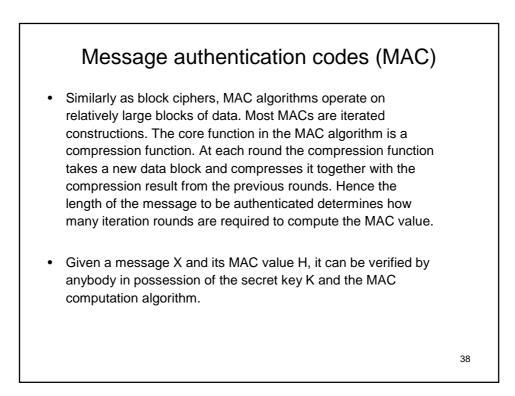


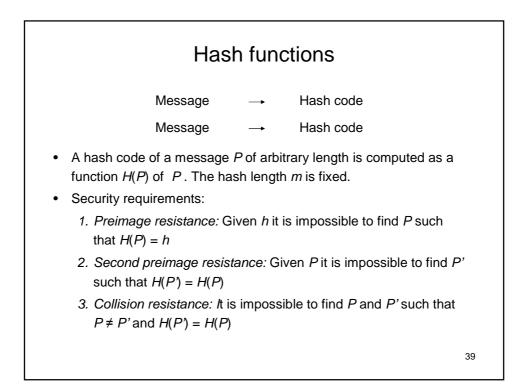


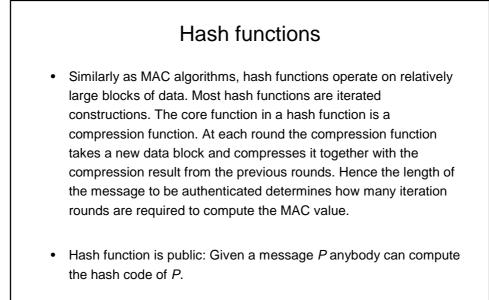


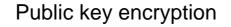












(Message , Public key) → Ciphertext

(Ciphertext , Private key) → Message

- Slow, usually used to encrypt short messages in more complex protocols than just bulk message encryption: authentication, key agreement etc.
- Because of the mathematics involved, complex message formatting rules (with hash functions) are required.
- Chosen ciphertext attacks maybe an essentially more serious threat than chosen plaintext (for symmetric block ciphers they are about the same). We will see an example later.
- RSA, ElGamal in different groups, Pairing based techniques ...

