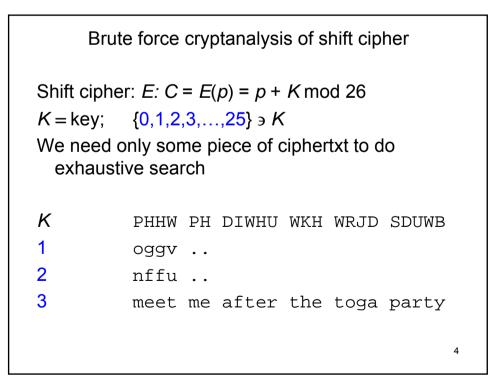


 $p = \text{plaintext letter}, \quad \{0, 1, 2, \dots, 25\} \ni p$   $C = \text{ciphertext letter}, \{0, 1, 2, \dots, 25\} \ni C$ Caesar substitution *E E*: *C* = *E*(*p*) = (*p* + 3) mod 26 0 -> 3; 1 -> 4; ... 22 -> 25; 23 -> 0; 24 -> 1; 25 -> 2 Caesar substitution, inverse transformation *D D*: *p* = *D*(*C*) = (*C* - 3) mod 26 0 -> 23; 1 -> 24; 2-> 25; 3 -> 0; ...; 25 -> 22



## Monoalphabetic substitution

Alphabets

Plain: abcdefghijklmnopqrstuvwxyz

Cipher: ABCDEFGHIJKLMNOPQRSTUVWXYZ

Key = permutation of the 26 characters

Size of key space 26!  $\cong$  4 x 10<sup>26</sup>

Cryptanalysis based on statistical properties of the plaintext

		of Letters in		
А	8.167	N	6.749	
В	1.492	0	7.507	
С	2.782	Р	1.929	
D	4.253	Q	0.095	
Е	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	x	0.150	
L	4.025	Y	1.974	
M	2.406	Z	0.074	

Cipherte	ext obtaine	ed from a	Substitut	ion Cipher	
~	MZRWQ				
	VEJBT ZKCEY				
~	NMXZN				
YIFZW	DYVZV	YFZUM	RZCRW	NZDZJ	
JXZWG	CHSMR	NMDHN	CMFQC	HZJMX	
JZWIE	JYUCF	WDJNZ	DIR		
					7

	riequ	ency ta		
A	0	N	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	
I	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\} \rightarrow D(D)

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

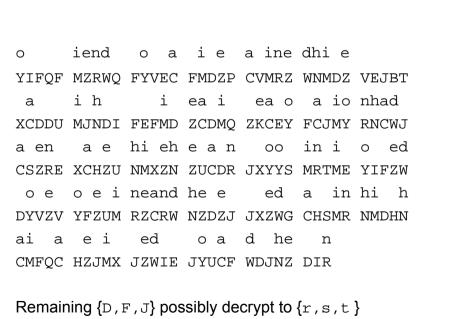
frequent we guess D(R) = n
```

10

#### Now we have end e ne dh e YIFOF MZRWO FYVEC FMDZP CVMRZ WNMDZ VEJBT h е е nh d XCDDU MJNDI FEFMD ZCDMQ ZKCEY FCJMY RNCWJ е h eh n en 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 ed d he е n CMFQC HZJMX JZWIE JYUCF WDJNZ DIR ne\_ndhe suggests that D(C) = a11

end e a ne dh а е YIFOF MZRWO FYVEC FMDZP CVMRZ WNMDZ VEJBT h ea ea а nhad а XCDDU MJNDI FEFMD ZCDMQ ZKCEY FCJMY RNCWJ eh a en a e h a n n ed CSZRE XCHZU NMXZN ZUCDR JXYYS MRTME YIFZW е е neand he e ed а n h h DYVZV YFZUM RZCRW NZDZJ JXZWG CHSMR NMDHN ed d he а е а n а CMFQC HZJMX JZWIE JYUCF WDJNZ DIR nh\_ decrypts to RNM suggests that D(M) = i or o 12

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



### Remaining $\{D, F, J\}$ possibly decrypt to $\{r, s, t\}$

ro a rise orr iend a ine dhise t YIFOF MZRWO FYVEC FMDZP CVMRZ WNMDZ VEJBT ass iths r ris easi ea rati nhadt XCDDU MJNDI FEFMD ZCDMO ZKCEY FCJMY RNCWJ аe hi eh asn t oo in i o red a en CSZRE XCHZU NMXZN ZUCDR JXYYS MRTME YIFZW re i neand heset ed а in his h so e DYVZV YFZUM RZCRW NZDZJ JXZWG CHSMR NMDHN eti ted air a to ar dsthe s n CMFOC HZJMX JZWIE JYUCF WDJNZ DIR

15

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

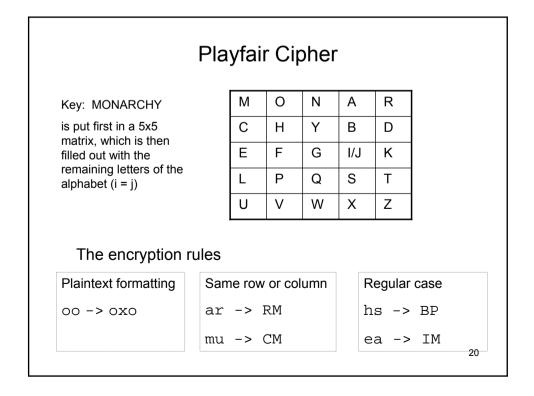
orfr iendf ro a rise a ine dhise t. YIFOF MZRWO FYVEC FMDZP CVMRZ WNMDZ VEJBT iths r ris easif ea o ratio nhadt ass XCDDU MJNDI FEFMD ZCDMQ ZKCEY FCJMY RNCWJ аe hi eh asn t oo in i o red a en CSZRE XCHZU NMXZN ZUCDR JXYYS MRTME YIFZW ore i neand heset ed in his h so e а DYVZV YFZUM RZCRW NZDZJ JXZWG CHSMR NMDHN airfa eti ted to ar dsthe s n CMFQC HZJMX JZWIE JYUCF WDJNZ DIR

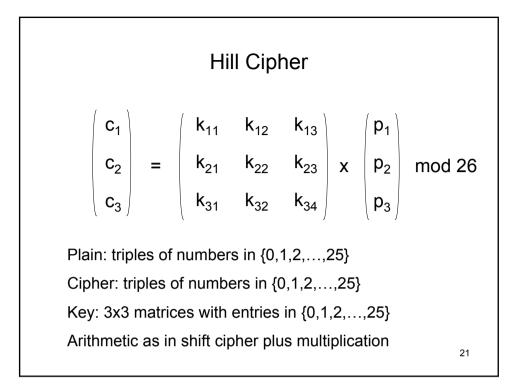
ourfr iendf ro a rise a ine dhise t. YIFOF MZRWO FYVEC FMDZP CVMRZ WNMDZ VEJBT ass ithsu r ris easif ea o ratio nhadt XCDDU MJNDI FEFMD ZCDMO ZKCEY FCJMY RNCWJ a e hi eh e asn t oo in i oured a en CSZRE XCHZU NMXZN ZUCDR JXYYS MRTME YIFZW so e ore i neand heset t ed a in his h DYVZV YFZUM RZCRW NZDZJ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

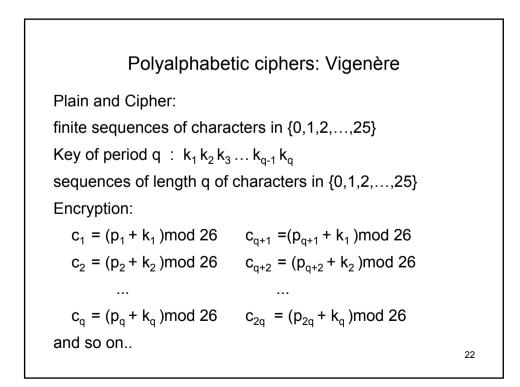
17

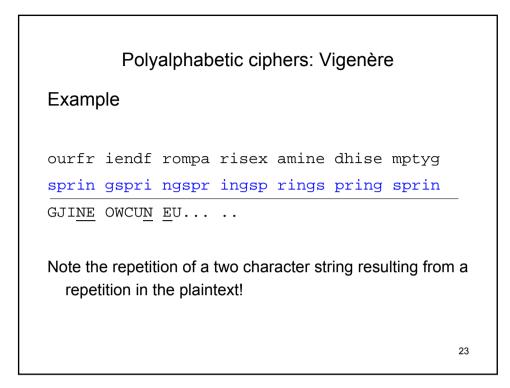
ourfr iendf rom a rise amine dhise m t YIFQF MZRWQ FYVEC FMDZP CVMRZ WNMDZ VEJBT ass ithsu r ris easif ea o ratio nhadt XCDDU MJNDI FEFMD ZCDMQ ZKCEY FCJMY RNCWJ a en a e hi eh e asn t oo in i oured CSZRE XCHZU NMXZN ZUCDR JXYYS MRTME YIFZW somem ore i neand heset t ed a in his h DYVZV YFZUM RZCRW NZDZJ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

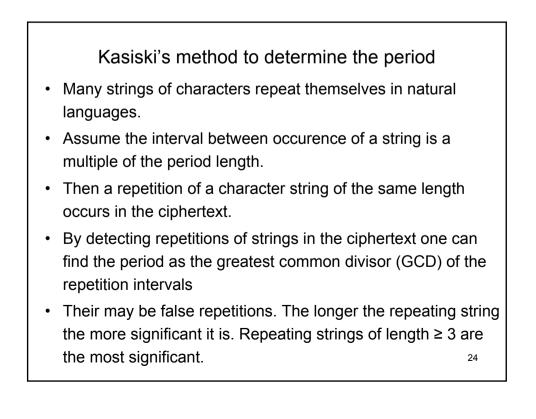
ourfriendfromparisexaminedhisemptygYIFQFMZRWQFYVECFMDZPCVMRZWNMDZVEJBTlasswithsurpriseasifevaporationhadtXCDDUMJNDIFEFMDZCDMQZKCEYFCJMYRNCWJakenplacewhilehewasntlookingipouredCSZREXCHZUNMXZNZUCDRJXYYSMRTMEYIFZWsomemorewineandhesettledbackinhischDYVZVYFZUMRZCRWNZDZJJXZWGCHSMRNMDHNairfacetilteduptowardsthesunCMFQCHZJMXJZWIEJYUCFWDJNZDIR

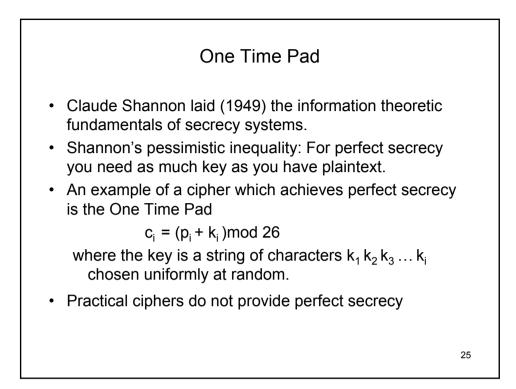


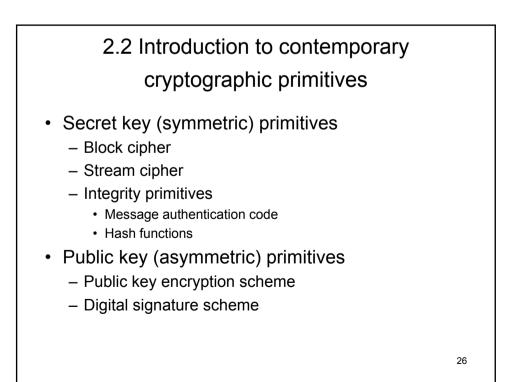


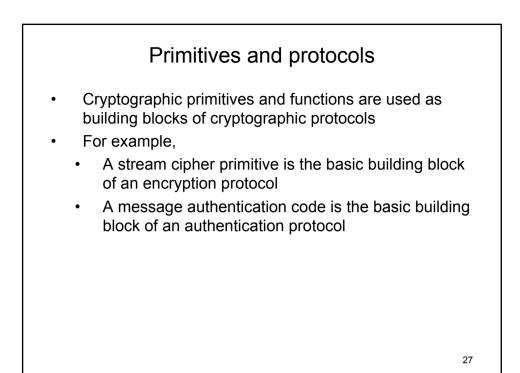


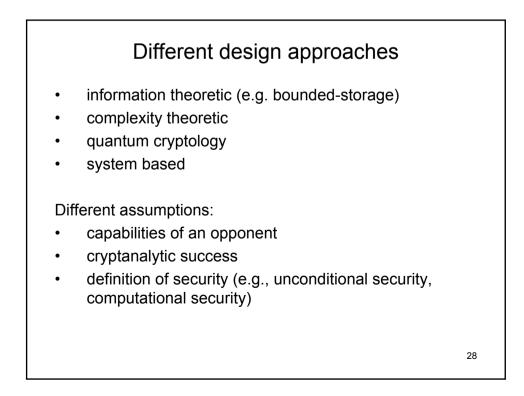












# Man-made vs. Math-made

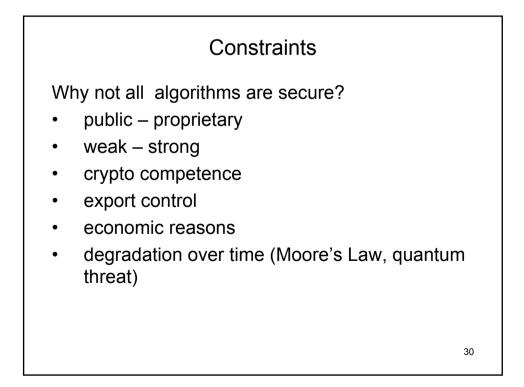
Symmetric primitives are

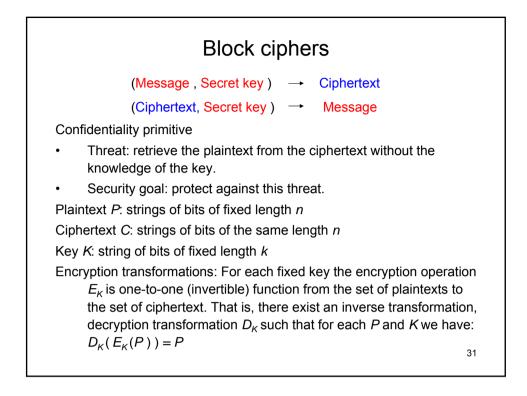
- based on man-made constructions.
- Fast and easy to implement in software and/or hardware
- Short keys

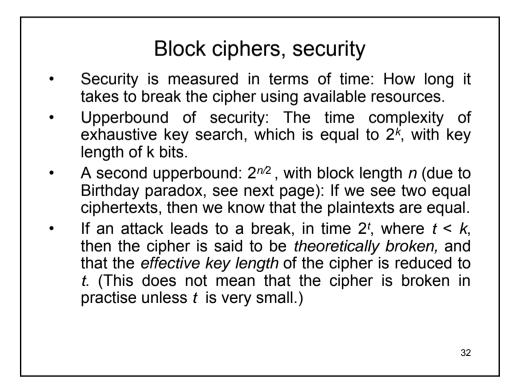
Asymmetric (public key primitives) are

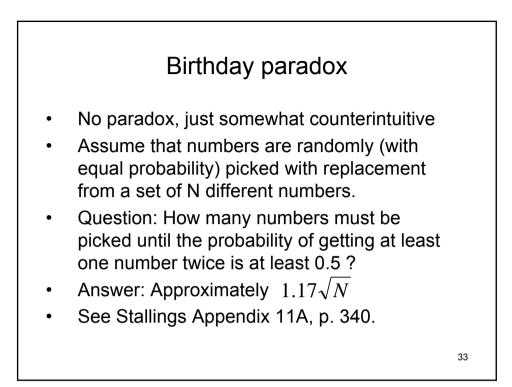
- Based on mathematical construction and their security is derived from infeasibility of some computationally hard problem.
- Slow and difficult to implement (both in software and hardware)
- Long keys and parameters

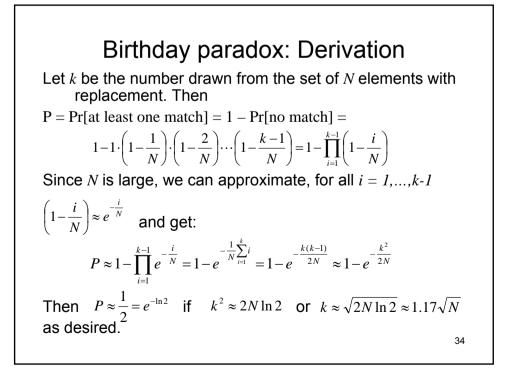
Note: it would be possible to construct symmetric primitives based on mathematics, but they are not used in practise because they are not efficient compared to symmetric primitives











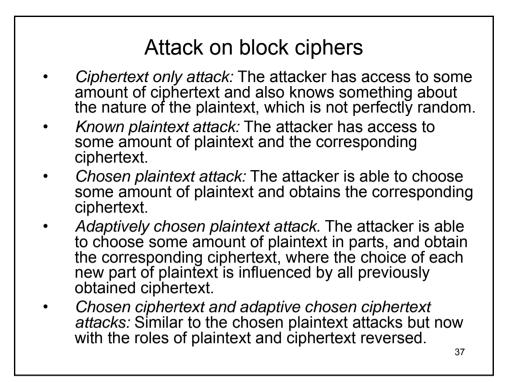
# Attack on block ciphers

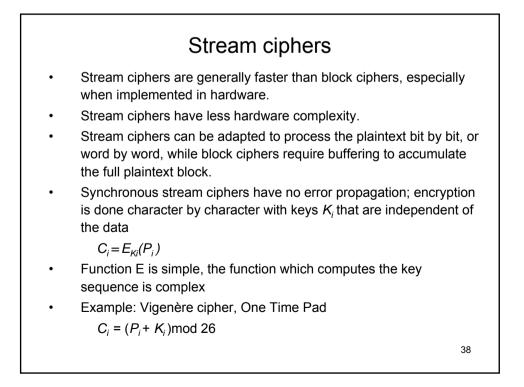
Let *n* be the block length in bits. Then if the block cipher encryption operation is used about  $2^{n/2}$  plaintexts times with the same key on any randomly generated data as plaintext, then by Birthday Paradox, the probability of having two equal ciphertexts is about  $\frac{1}{2}$ . Then one knows that the two corresponding input data are equal.

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

36



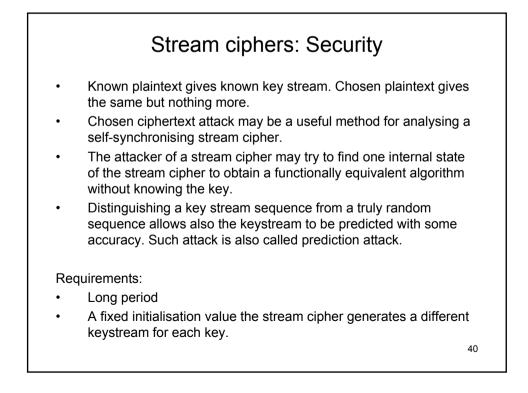


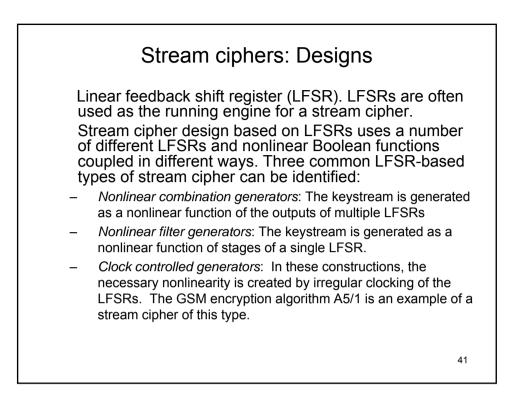
# Stream cipher encryption

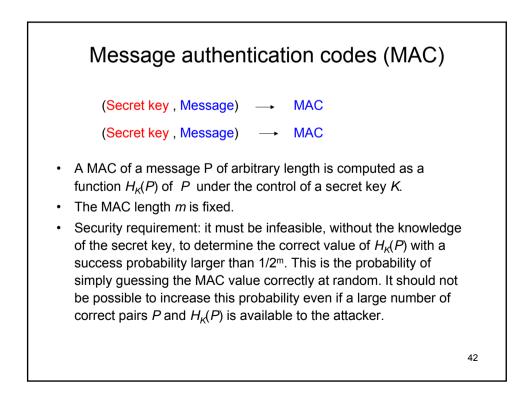
Secret key  $\rightarrow$  Key stream (Key stream, Message)  $\rightarrow$  Ciphertext

Secret key  $\rightarrow$  Key stream (Ciphertext, Key stream )  $\rightarrow$  Message



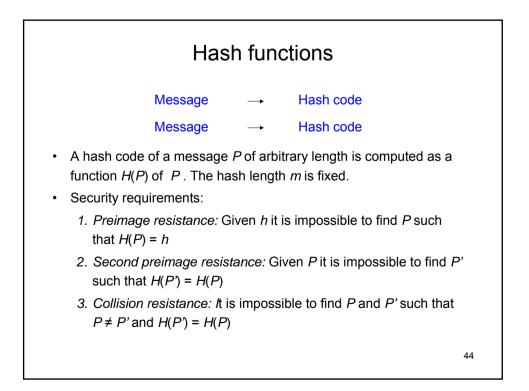






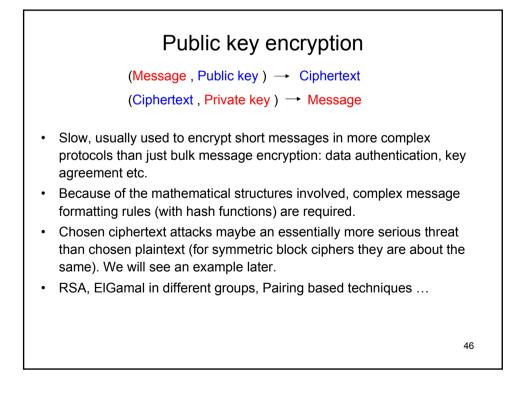
# Message authentication codes (MAC)

- Similarly as block ciphers, MAC algorithms operate on relatively large blocks of data. Most MACs are iterated constructions. The core function in the MAC algorithm is a compression function. At each round the compression function takes a new data block and compresses it together with the compression result from the previous rounds. Hence the length of the message to be authenticated determines how many iteration rounds are required to compute the MAC value.
- Given a message X and its MAC value H, it can be verified by anybody in possession of the secret key K and the MAC computation algorithm.



# Hash functions

- Similarly as MAC algorithms, hash functions typically operate on relatively large blocks of data. Most hash functions are iterated constructions. The core function in a hash function is a compression function. At each round the compression function takes a new data block and compresses it together with the compression result from the previous rounds. Hence the length of the message to be authenticated determines how many iteration rounds are required to compute the MAC value.
- Hash function is public: Given a message *P* anybody can compute the hash code of *P*.



# **Digital signatures**

(Message , Private key )  $\rightarrow$  Signature (Signature , Public key )  $\rightarrow$  Validity (1 bit)

- Important primitive; the only one to provide non-repudiation.
- Slow, message are signed by applying the digital signature operation on a fixed length hash of the message.
- Used for
  - message authentication protocols
  - non-repudiation protocols
  - authentication and key agreement
  - commitment schemes
  - ...
- RSA, ElGamal in different groups, Schnorr, DSA, Pairing based techniques