Cryptography:
Information confidentiality, integrity, authenticity, person identification

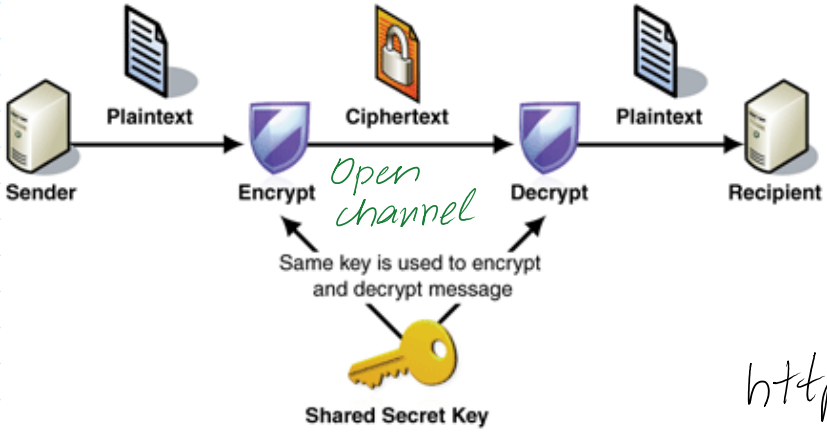
Symmetric cryptography ---------- Asymmetric cryptography

Symmetric encryption
H-functions, Message digest
HMAC H-Message Authentication Code

$P(1\ move) = 1/2$
$10\ moves \longrightarrow 2^{10} = 1024$
$P(10\ moves) = 1/1024$

Asymmetric encryption
E-signature - Public Key Infrastructure - PKI
Data authenticity
Person identification
E-money
E-voting
Digital Rights Management - DRM
Etc.

Symmetric encryption



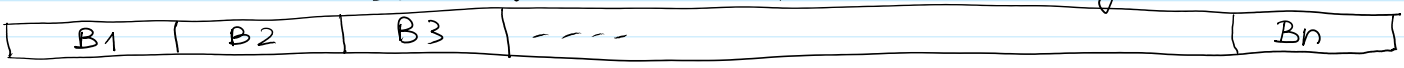
https:/ KAP

AES - 128, 192, 256 Block cipher --> Encryption --> Decryption

Advanced Encryption Standard ~ 2000

Key length 128, 192, 256 bits: $k \in \{128b, 192b, 256b\}$

Data to be encripted : message m



The length of any block Bi should be $|B_i| = 128$ bits
192 bits
$|B_1| = |B_i|$

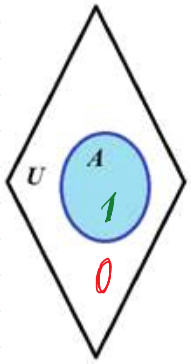
The length of any block B_i should be $|B_i| = 128$ bits
$|B_i| = |k|$ 192 bits
256 bits

$Enc_{AES}(k, B1) = C1$
$Enc_{AES}(k, B2) = C2$
$Enc_{AES}(k, Bn) = Bn$

$Enc_{AES}(k, m) = c \xrightarrow{\quad c \quad} Dec_{AES}(k, c) = m$

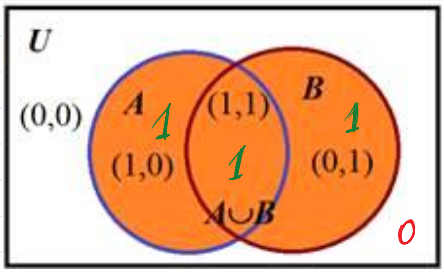
Vernam cipher (1917) - One Time Pad

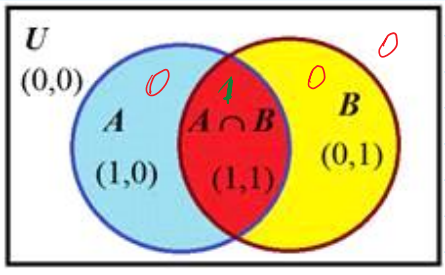
Logical operations

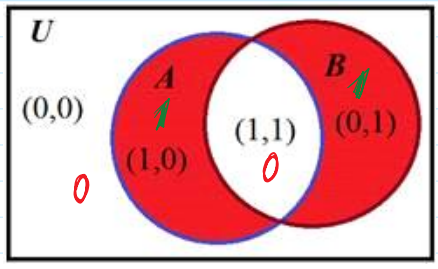


dart

$A \cup B$ $A \cap B$ $A \oplus B$







„0" No
„1" Yes

$m \in \{0,1\}$

$k \leftarrow rand\{0,1\}$; $k \in \{0,1\}$

$c = m \oplus k$

$Pr(k=0) = 1/2$
$Pr(k=1) = 1/2$

$\xrightarrow{\quad c \quad}$

if $c=0$
if $c=1$
} eavesdropping adversary

A	B	$A \oplus B$
0	0	0
0	1	1
1	0	1
1	1	0

m	k	$m \oplus k = c$
0	0	0
0	1	1
1	0	1
1	1	0

$c - k = m$

$\oplus$ – is inverse to itself

$c = m \oplus k - k = m$

$c = m \oplus k \oplus k =$

$= m \oplus 0 = m = 1$

Alice: $k = 1$.

Let $m = 1$; $k = 1$: $Pr(k=1) = 1/2$

$c = m \oplus k = 1 \oplus 1 = 0$ $\xrightarrow{c=0}$ Bob: $k = 1$.

$c \oplus k = 0 \oplus 1 = 1 = m$.

But nevertheless, the reader confusing implication and equivalence operations (functions) can accept the following proposition as valid:
if talker has a head and donkey has a head, then talker is a donkey.
To accept this proposition as valid means that thinker confuses notions of implication and equivalence. If reader is afraid to make such a mistake, we recommend to read about that in any external source.

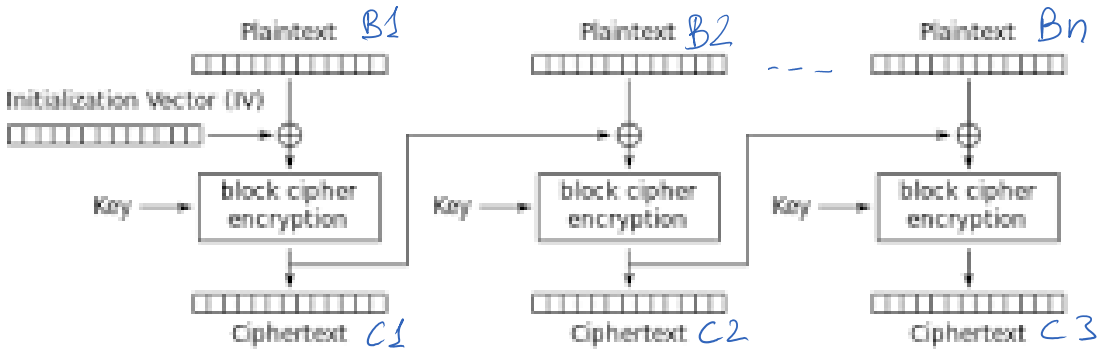
```
>> m=77000
m =  77000
>> mb=dec2bin(m)
mb = 10010110011001000
```

message m consist of 17 bits : $|m| = 17$ bits.

Symmetric encryption

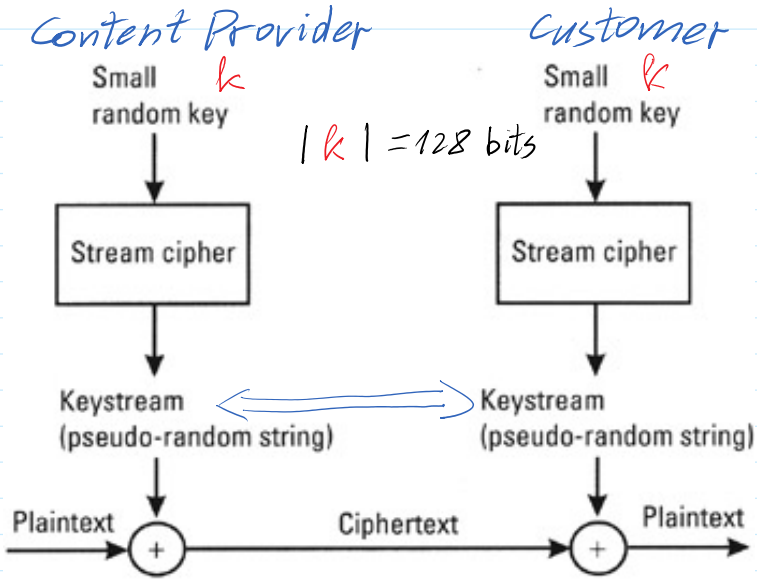
- **block cipher** is one in which a block of plaintext is treated as a whole and used to produce a cipher text block of equal length.

in which message (plain text) of any finite length is divided into the number of same length block and every block is encrypted with the same relatively short key of length 128 bits, 192 bits, 256 bits or the similar length



Cipher Block Chaining (CBC) mode encryption

AES-128-CBC : $|B1| = |B2| = \dots = |Bn| = 128$ bits



- A **stream cipher** is one that encrypts a digital data stream one bit or one byte at a time. Examples of classical stream ciphers are the auto keyed Vigenère cipher and the Vernam cipher.