

Il sistema numerico decimale

Il sistema numerico decimale

- Il sistema numerico di uso corrente è decimale e posizionale;
- Decimale perchè formato da 10 cifre:
0, 1, 2, 3, 4, 5, 6, 7, 8, 9;
- Posizionale perchè il valore di ogni cifra nel numero si ottiene moltiplicando la cifra per una potenza del 10 (10^0 , 10^1 , 10^2 , 10^3 ...) a seconda della posizione occupata nel numero, a partire da destra;
- Il valore del numero si ottiene sommando tutte le cifre ognuna moltiplicata per il proprio peso.

Pesi decimali

Posizione (destra verso sinistra!)	Quinta	Quarta	Terza	Seconda	Prima
Peso	10^4 (10'000)	10^3 (1'000)	10^2 (100)	10^1 (10)	10^0 (1)

Esempi di numeri decimali (1/2)

4067	4	0	6	7	Cifre
	1000	100	10	1	Pesi
	4'000	0	60	7	Risultato
	+				
	4067				

Esempi di numeri decimali (2/2)

2222	2	2	2	2	Cifre
1000	100	10	1	Pesì	
2'000	200	20	2	Risultato	
+					
2222					

Sistema numerico romano: un sistema non posizionale!

Un paragone storico

Sistema numerico romano:

Additivo ma non posizionale!

Al posto di dieci cifre innumerevoli simboli:

I=>1, V=> 5, X=>10, C=>100,

D=> 500, M=>1000

XXII = 10 + 10 + 1 + 1 = 22

Il sistema numerico binario

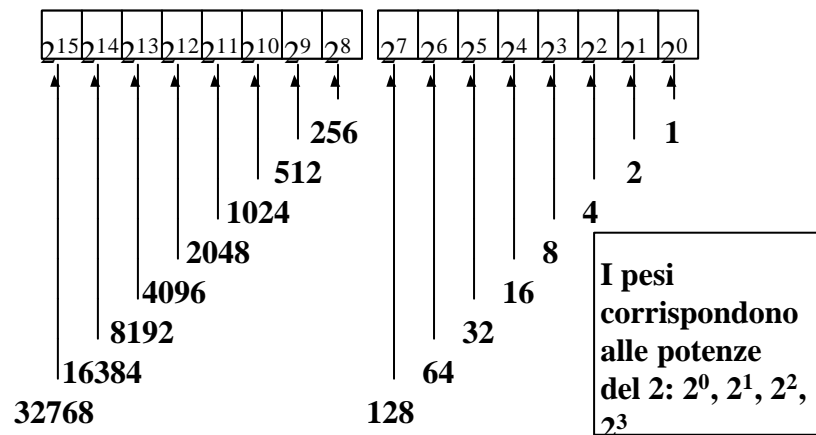
Il sistema numerico binario

- E' il sistema numerico adoperato dai calcolatori elettronici e da molti altri sistemi digitali;
- Binario perchè formato da 2 cifre: 0, 1 (si usa il termine bit, abbreviazione di BInary digiT);
- Posizionale perchè il valore di ogni cifra nel numero si ottiene moltiplicando la cifra per una potenza del 2 (2^0 , 2^1 , 2^2 , $2^3...$) a seconda della posizione occupata nel numero, a partire da destra;
- Il valore del numero si ottiene sommando tutte le cifre ognuna moltiplicata per il proprio peso.

Pesi binari (1/2)

Posizione (destra verso sinistra!)	Quinta	Quarta	Terza	Seconda	Prima
Peso	2^4 (16)	2^3 (8)	2^2 (4)	2^1 (2)	2^0 (1)

Pesi binari (2/2)



Esempi di numeri binari (1/2)

1101

1	1	0	1	Cifre
8	4	2	1	Pesi
8	4	0	1	Risultato

+

13 (espresso come numero
decimale)

Esempi di numeri binari (2/2)

0111

0	1	1	1	Cifre
8	4	2	1	Pesi
0	4	2	1	Risultato

+

7 (espresso come numero
decimale)

Il sistema numerico esadecimale

Il sistema numerico esadecimale

- Esadecimale (dal greco sedici) perchè formato dalle cifre decimali (0, 1, 3, 4, 5, 6, 7, 8, 9) e dalle cifre A, B, C, D, E, F per i numeri da 10 a 15;
- Posizionale perchè il valore di ogni cifra nel numero si ottiene moltiplicando la cifra per una potenza del 16 (16^0 , 16^1 , 16^2 , $16^3...$) a seconda della posizione occupata nel numero, a partire da destra;
- Il valore del numero si ottiene sommando tutte le cifre ognuna moltiplicata per il proprio peso.

Pesi esadecimali

Posizione (destra verso sinistra!)	Quinta	Quarta	Terza	Seconda	Prima
Peso	16^4 (65'536)	16^3 (4'096)	16^2 (256)	16^1 (16)	16^0 (1)

Esempi di numeri esadecimali

(1/2)

100A

1	0	0	A	Cifre
$4'096$	256	16	1	Pesi
$4'096$	0	0	10	Risultato
+				

$4'106$ (espresso come numero
decimale)

Esempi di numeri esadecimali

(2/2)

3471

3	4	7	1	Cifre
4'096	256	16	1	Pesi
12'288	1'024	112	1	Risultato

+

13'425 (espresso come numero
decimale)

Trasformazioni tra sistemi numerici

Paragone dei tre sistemi

Decimale	Binario	Esadecimale
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5
6	0110	6
7	0111	7
8	1000	8
9	1001	9
10	1010	A
11	1011	B
12	1100	C
13	1101	D
14	1110	E
15	1111	F

Passaggio dal sistema binario al sistema decimale (1/2)

- Si moltiplicano le cifre binarie ciascuna per il proprio peso e si sommano

Passaggio dal sistema binario al sistema decimale (2/2)

1101

1	1	0	1	Cifre
8	4	2	1	Pesi
8	4	0	1	Risultato

+

13 (numero decimale)

Passaggio dal sistema decimale al sistema binario (1/2)

- Si divide il numero decimale ripetutamente per 2 fino ad ottenere il quoziente 0 e si considerano i resti ottenuti.
 - La sequenza dei resti costituisce il numero espresso in cifre binarie;

Passaggio dal sistema decimale al sistema binario (2/2)

47

47	:2	=	23	1
23	:2	=	11	1
11	:2	=	5	1
5	:2	=	2	1
2	:2	=	1	0
1	:2	=	0	1

101111

Verifica

$$1 \times 32 + 0 \times 16 + 1 \times 8 + 1 \times 4 + 1 \times 2 + 1 \times 1 = 47$$

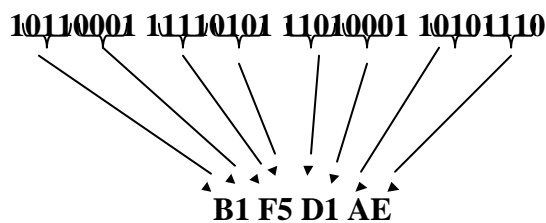
Passaggio dal sistema binario al sistema esadecimale (1/3)

- Si raggruppano le sequenze di cifre binarie in gruppi di 4 a partire dalla destra (queste sequenze hanno valori numerici tra 0 e 15);
- Si sostituisce ad ogni valore numerico la corrispondente cifra esadecimale;

Passaggio dal sistema binario al sistema esadecimale (2/3)

Insieme 4 bit	Cifra esadecimale	Valore
0000	0	0
0001	1	1
0010	2	2
0011	3	3
0100	4	4
0101	5	5
0110	6	6
0111	7	7
1000	8	8
1001	9	9
1010	A	10
1011	B	11
1100	C	12
1101	D	13
1110	E	14
1111	F	15

Passaggio dal sistema binario al sistema esadecimale (3/3)



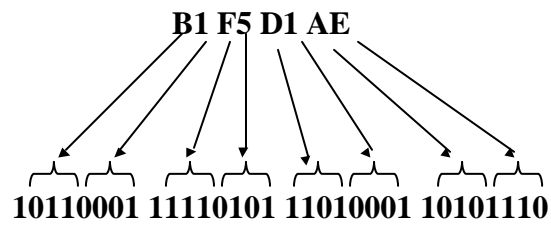
Passaggio dal sistema esadecimale al sistema binario (1/3)

- Si sostituisce ad ogni valore esadecimale la corrispondente quaterna di cifre binarie, iniziando come sempre a destra;

Passaggio dal sistema esadecimale al sistema binario (2/3)

Insieme 4 bit	Cifra esadecimale	Valore
0000	0	0
0001	1	1
0010	2	2
0011	3	3
0100	4	4
0101	5	5
0110	6	6
0111	7	7
1000	8	8
1001	9	9
1010	A	10
1011	B	11
1100	C	12
1101	D	13
1110	E	14
1111	F	15

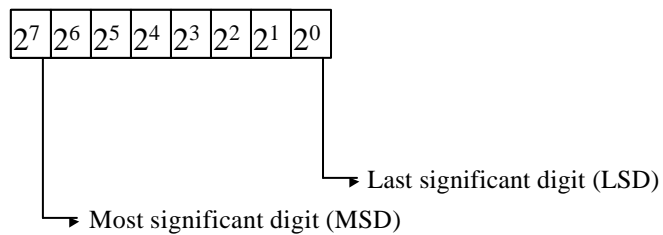
Passaggio dal sistema esadecimale al sistema binario (3/3)



Considerazioni su bit e byte

Il byte (1/2)

- Il byte rappresenta l'insieme di 8 bits (a volte si incontra il termine ottetto);



Il byte (2/2)

- Un byte (8 bit) può assumere 256 (2^8) differenti valori:
 - Un bit può assumere 2 valori [0,1];
 - Due bit possono assumere 4 valori [00, 01, 11, 10];
 - Tre bit possono assumere 8 valori [000, 001, 010, 011, 100, 101, 110, 111];
 - Otto bit possono assumere 256 valori [00000000...11111111];
- Più in generale una sequenza di n bit può assumere 2^n differenti valori.

Multipli del bit e del byte (1/5)

- Per indicare in maniera sintetica grandezze fisiche molto grandi si usano i termini:
 - Kilo per 1'000 (un migliaio di unità);
 - Mega per 1'000'000 (un milione di unità);
 - Giga per 1'000'000'000 (un miliardo di unità);
- Esse sono radicate nell'uso del dieci nella fisica e nelle scienze esatte in generale;

Multipli del bit e del byte (2/5)

- In informatica dove si opera in termini binari si preferiscono delle definizioni differenti, basate sull'uso di potenze del 2:
 - Kilo per indicare 1'024 (2^{10});
 - Mega per indicare 1'048'576 (2^{20});
 - Giga per 1'073'741'824 (2^{30});

Multipli del bit e del byte (3/5)

	Fisica	Informatica
Kilo	1'000 (10^3)	1'024 (2^{10})
Mega	1'000'000 (10^6)	1'048'576 (2^{20})
Giga	1'000'000'000 (10^9)	1'073'741'824 (2^{30})

Multipli del bit e del byte (4/5)

KBit (KB)	1'024 Bit
Mbit (MB)	1'048'576 Bit (circa un milione di Bit)
Gbit (GB)	1'073'741'824 Bit (circa un miliardo di Bit)

Multipli del bit e del byte (5/5)

KByte	1'024 Byte
MByte	1'048'576 Byte (circa un milione di Byte)
GByte	1'073'741'824 Byte (circa un miliardo di Byte)

I codici

I codici per rappresentare i caratteri

- Codice ASCII (American Standard Code for Information Interchange);
 - 8 bit per rappresentare nel calcolatore caratteri e per simboli speciali;

La crittografia

Cifrare (1/4)

- Mediante la cifratura un testo (“testo in chiaro”) viene trasformato in un “testo cifrato”;
- La cifratura viene fatta usando procedimenti di grande complessità matematica ma che possono essere ricondotti all’uso di una chiave;
- Il testo puo’ essere decifrato solo da chi è in possesso del cifrario cioè della chiave;

Cifrare (2/4)

- Giulio Cesare pare abbia usato un codice che sostituiva ad ogni cifra quella che veniva 3 posti dopo nell’alfabeto :
– a -> D, b -> E, c -> F,...z->C;
- Con il cifrario “Giulio Cesare” la parola “attacco” diventa “DWWDFFR”;
- Un altro esempio di cifrario è sul lucido (3/4)

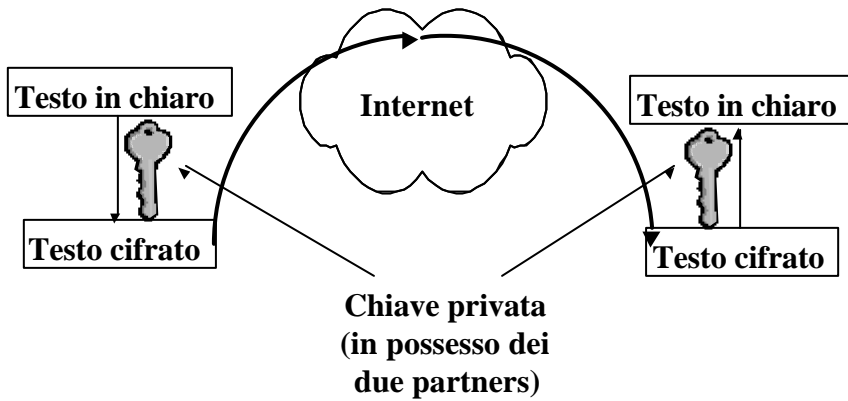
Cifrare (3/4)

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

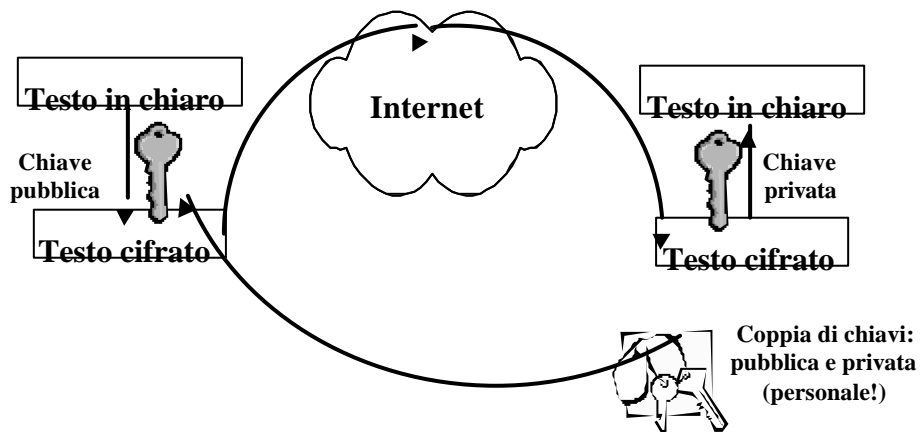
Cifrare (4/4)

- Con il cifrario della slide (3/4) la parola “attacco” diventa “QZZQEEG”;

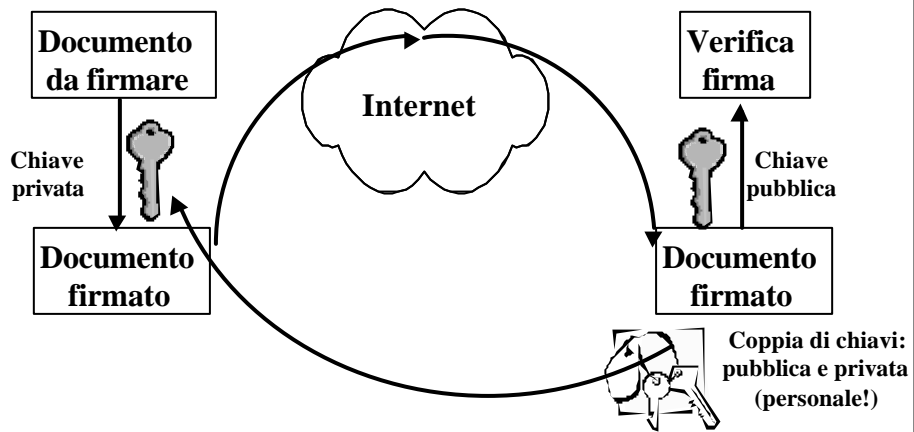
Cifratura a chiave privata (simmetrica)



Cifratura a chiave pubblica (asimmetrica)



Cifratura a chiave pubblica: la firma digitale



Gli operatori logici

Operazioni logiche

- Le operazioni logiche operano su singoli bit;
- Le operazioni logiche piu' usate sono AND, OR, XOR, NOT;
- Le operazioni logiche sono definite per il tramite di "tavole di verità".

AND

Ingresso A	Ingresso B	Uscita
0	0	0
0	1	0
1	0	0
1	1	1

OR

Ingresso A	Ingresso B	Uscita
0	0	0
0	1	1
1	0	1
1	1	1

XOR

Ingresso A	Ingresso B	Uscita
0	0	0
0	1	1
1	0	1
1	1	0

NOT

Ingresso	Uscita
0	1
1	0

Mascheramento (masking)

- Operazione di AND tra una maschera prefissata ed una sequenza binaria:

Maschera	→	1111 1111 0000 0000	} AND
Sequenza binaria	→	1010 0010 1100 0101	
		1010 0010 0000 0000	

Gli insiemi

Insiemi (1/3)

- Da un punto di vista matematico è un concetto “primitivo”, che non può essere ulteriormente definito;
- Sinonimi di “insieme” nel linguaggio ordinario sono termini come “famiglia” o “collezione” di oggetti;

Insiemi (2/3)

- Esempi di insiemi:
 - Insieme numeri pari su facce dado {2, 4, 6};
 - Insieme numeri dispari su facce dado {1, 3, 5};
 - Insieme semi carte napoletane: {ori, bastoni, spade, coppe};
 - Insieme numeri interi {1, 2, 3, };

Insiemi (3/3)

- Importanti definizioni:
 - I componenti di un insieme sono detti “elementi” dell’insieme;
 - “Cardinalità” di un insieme e’ il numero degli oggetti facenti parte di un insieme

Osservazione importante:
Esistono insiemi finiti (formati da un numero finito di elementi) e insiemi infiniti.

Operazioni sugli insiemi (1/4)

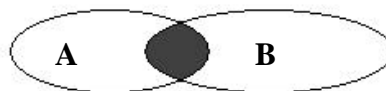
- Unione di due insiemi:
Insieme formato dagli elementi che appartengono all'uno o all'altro insieme



$A \cup B$

Operazioni sugli insiemi (2/4)

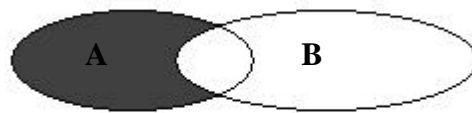
- Intersezione di due insiemi:
Insieme formato dagli elementi che appartengono ad ambedue gli insiemi



$A \cap B$

Operazioni sugli insiemi (3/4)

- Differenza di due insiemi:
elementi che appartengono ad A ma non contemporaneamente ad A e B



$A - B$

Operazioni sugli insiemi (4/4)

- Differenza simmetrica di due insiemi:
elementi che appartengono ad A o B ma non contemporaneamente ad A e B



$A \Delta B$

Compressione

- Comprimere un file significa ridurre lo spazio di memoria occupato da un file;
- Gli algoritmi di compressione sfruttano tecniche matematiche sofisticate ma il principio è semplice: sfruttare la struttura dei dati (ridondanza dell'informazione);
- Compressione puo' essere utilizzato all'interno di un disco rigido o ad esempio per inviare allegati di una e-mail.