

Sistemi Operativi

Leonardo Mengozzi

Titoletti indice link a rispettive sezioni, in alto a sinistra "←Indice" link a pagina Indice.

Contents

1 Bash	2
Comandi Variabili	2
Comandi File speciali	2
Comandi Directory	2
Comandi Controllo Comandi	2
Comandi Scripting	3
Comandi Espressioni aritmetica	4
Comandi Espressioni condizionali	4
Comandi Tilde Expansion	5
Comandi Privilegi	5
Comandi Subshell	5
Comandi Uso File Descriptor	6
Comandi Standard input e output	7
Comandi Utilities	7
Comandi Process Identifier	8
Comandi Vari	10
Comandi Costrutti controllo flusso	10
2 Crittografia	10
2.1 Crittografia Simmetrica (chiave segreta)	10
2.2 Crittografia Asimmetrica (chiave pubblica)	11
2.2.1 Funzioni Hash Crittografiche	11
2.3 MAC e Firma digitale	12
2.4 GPG e PGP	12
3 Programmazione Concorrente	12
Comandi Multi-processo	12
Comandi PIPE	13
Comandi Multi-thread	13
3.1 SJF	14
3.2 Produttore e consumatore	14
3.3 Buffer limitato	15
3.4 Filosofi orientali a cena	16
3.5 Message Passing	17
3.6 Concorrenza in C	17
Comandi Funzioni semafori	17
4 Esercizi Scheduling	18
5 File Descriptors	18
6 Risorse	19
6.1 Grafo di Holt Generale (classi e processi)	19
6.2 Detaction and recovery - Caaso 1	19
6.3 Detaction and recovery - Caaso 2	20
6.4 Detaction and recovery - Knot	20
6.5 Stato SAFE - algoritmo del banchiere	20

7 Gestione Pacchetti in Linux	20
7.1 Concetti chiave	20
7.2 Installazione Package	20
7.2.1 Posizione Repository	21

1 Bash

Variabili	Descrizione
PATH	V. Ambiente: Modificabile, sequenza di percorsi assoluti, divisi da ":" , di directory contenenti eseguibili (lanciabili senza digitare path). Ricerca secondo ordine specificato in PATH, si ferma a primo eseguibile con nome uguale. Eventuale ErrorNotFound. Altre variabili d'ambiente: \$HOME, \$USER, \$SHELL, \$TERM.
env	Visualizza l'elenco delle variabili d'ambiente.
IFS=\$' \t \n'	Contiene caratteri separatori delle parole negli elenchi.
/dev/null	File speciale che scarta tutto quello che gli viene scritto.
LC_CTYPE	Imposta il tipo locale dei caratteri. Usata da cut e ws per capire numero byte caratteri.

File speciali	Descrizione
/etc/passwd	Righe sono info ogni utente divise da ":".
/etc/shadow	Righe sono password utente codificate.
/etc/group	Righe sono info ogni gruppo divise da ":".
/usr/bin/passwd	Cambia la pass utente.

Directory	Descrizione
cd <i>percorso</i>	Sposta logicamente in una diversa directory, secondo un path assoluto o relativo.
mkdir <i>nomeDir</i>	Crea una nuova directory.
touch <i>nomeFile.estensione</i>	Crea un file vuoto nella directory corrente.
rmdir <i>nomeDir</i>	Rimuove una directory solo se è vuota.
rm <i>file dir</i>	Rimuove una directory vuota o un file. Parametri: <ul style="list-style-type: none"> • -r elimina ricorsivamente sotto cartelle e file. • -f non fa chiedere le autorizzazioni di eliminazione.
mv <i>file1 file2 dir</i>	Rinomina file1 in file2 o sposta file1 nella directory specificata.
cp <i>file1 dir</i>	Copia file1 nella directory specificata.
ls [<i>nomefile</i>]	Visualizza i files/directory contenuti nella directory corrente. Parametri: <ul style="list-style-type: none"> • -a mostra anche file nascosti (anche .., ..). • -l mostra più informazioni sui files. • -h rende i dati più leggibili. • -d fa applicare il comando alla directory e non ai file. • -R mostra ricorsivamente contenuto sotto directory.
pwd	Se specifico un file mi dice se esiste e mi da informazioni solo di lui. Visualizza il percorso assoluto, da / fino alla directory corrente.

Controllo Comandi	Descrizione
\	Disabilita interpretazione per il carattere successivo, andata a capo, permettendo di stamparlo.
..."	Delimita un argomento e non fa interpretare nessun comando a eccezione dell'espansione di variabili (\$..) e l'esecuzione di comandi.
'...'	Delimita un argomento e non fa interpretare nessun comando.
\$'...'	Espande backslash-escaped direttamente nella stringa espansa in una single-qouted stringa. Backslash-escaped: \a, \e, \f, \r, \v, \', \b, \E, \n, \t, \\, \", \nnn, \xHH, \cn.
pre{\${s1,...}}post	Stringa di testo racchiusa fra separatori (spazio, tab, a capo) con coppia di graffe (non precedute da \$) e senza separatori. Le stringhe racchiuse dalle graffe vengono composte con il preambolo (pre) e postscritto (post), che sono opzionali. Alternative: Sono annidabili (quelle più esterne eseguite per prime). Vengono eseguite prima le brace expansions delle variable expansions.
	<ul style="list-style-type: none"> • $a_1..a_2$ lettere da a_1 a a_2 nell'alfabeto. • $n_1..n_2$ numeri compresi tra n_1 e n_2.
cmd1 ; ...	Separatore di più comandi, e dei rispettivi argomenti, scritti sulla stessa riga di comando e eseguiti dopo la terminazione del precedente (lista di comandi). L'exit status è quello dell'ultimo comando lanciato. Se racchiusi da () eseguiti in una sub-shell.
cmd1 cmd2	Esegue cmd1 e solo se cmd1 fallisce (exit status ≠ 0) esegue cmd2.
cmd1 && cmd2	Esegue cmd1 e solo se cmd1 ha successo (exit status = 0) esegue cmd2.
[...]]	Espressione condizionale, usa && e , che restituisce 0=true, altro=false.
*	Sostituito con una qualsiasi sequenza di caratteri anche vuota.
?	Sostituito con un singolo carattere (no spazio vuoto).
[c1c2...]	Sostituito con solo uno dei caratteri specificati in elenco. Alternative: <ul style="list-style-type: none"> • $a_1..a_2$ lettere da a_1 a a_2 nell'alfabeto. • $n_1..n_2$ numeri compresi tra n_1 e n_2. • [:digit:] una cifra. • [:upper:] un carattere maiuscolo. • [:lower:] un carattere minuscolo.
	Annidabili.

Scripting	Descrizione
<code>echo <i>testo</i></code>	Visualizza a video la sequenza di caratteri passata fino al primo "INVIO". Se passo " <i>testo</i> " si disabilita l'interpretazione dei caratteri speciali e andate a capo. <ul style="list-style-type: none"> • -e Stampa i caratteri speciali (\...). • -n Non fa andare a capo.
<code>nome=valore</code>	Simboli con nome e valore, stringa modificabile, alfanumerici casesensitive. No spazi prima o dopo "=" . Sono d'ambiente o ex-novo locali. Solo la bash in cui sono create le variabili le può usare. I programmi lanciati dalla bash hanno una speudocopia della bash.
<code>\$variabile</code>	Fa l'espansione della variabile, ovvero la sostituisce con il suo contenuto.
<code>#variabile</code>	Restituisce il numero di caratteri del contenuto della variabile.
<code> \${!variabile}</code>	Fa l'espansione della variabile che contiene il nome d'un'altra variabile con il valore di quest'ultima (riferimento indiretto).
<code>Dalla versione 2 di bash.</code>	
<code>export nomevar nomevar=valore</code>	Variabile d'ambiente. Un shell figlia riceve una copia modificabile che non influenza variabile d'ambiente del padre.
<code>unset nomevariabile</code>	Elimina una variabile esistente (vuota o no). Quotare ("...") sempre variabili per evitare errori con variabili vuote o inesistenti.
<code> \${nomeVar}</code>	Fa sostituire il nome della variabile con il valore. graffe opzionali se nome variabile seguito da uno spazio.
<code>#...</code>	Commetto.
<code>#!...</code>	Se indicato nella prima riga indica quale interprete deve eseguire lo script. Se non specificato usato quello corrente.
<code>comando1 comando2</code>	pipe (speudo-file temporaneo): collega automaticamente l'output di un comando all'input di un altro. Unidirezionale sinDes.
<code>script.sh c1...</code>	Sono un insieme ordinato di caratteri separati da spazi successivi al nome del programma. Sono immodificabili dopo la sostituzione dei metacaratteri (*, ?, ecc). Riga di comando = nomeProgramma + parametri. Nella riga di comando gli elementi sono indicizzati da 0 (nomeProgramma). <ul style="list-style-type: none"> • \$# Contiene il numero di parametri passati. • \$n Accede all'n-esimo parametro a partire da indice 0. • \$* Tutti argomenti concatenati e divisi da spazi. • \$@ Vettore di argomenti quotati ("...").
<code>'comando ./script.sh'</code>	I parametri \$* e \$@ sono identici se non quotati (concatenazione di argomenti separati da " "). Se quotati \$* quota tutti gli argomenti assieme mentre \$@ quota singolarmente ogni argomento. \$@ è usato per passare parametri a comandi dentro a degli script.
<code>Command substitution.</code>	Sostituisce (a run-time) nella riga in cui è specificato il comando o script con l'output (stdout). Comando alternativo <code>\$(./script.sh)</code>
<code>\$?</code>	Modificato alla terminazione di ogni script, contiene l' <i>exit status</i> .

Espressioni aritmetica	Descrizione
<code>((...))</code>	Valuta una stringa come un'espressione aritmetica (+,-,*,/,%,(,),!,&&,) di soli interi. Racchiude un'espressione più eventualmente un assegnamento. Si possono usare variabili nell'espressione (\$variabile). Exit statuts 0=true, altro=false. Non contiene espressioni condizionali e comandi.
<code>\$((...))</code>	Per le operazioni in virgola mobile usare bc . Come operatore ((...)) ma è concatenabile con stringhe tramite " ".

Espressioni condizionali	Descrizione
[[...]]	<p>Restituisce exit status 0=true, altro=false.</p> <ul style="list-style-type: none"> Non può contenere commandi, word splitting, brace expansion, pathname expansion. Non esegue assegnamenti a variabile, annidamenti di espressioni condizionali. Può contenere variable expansion, solo \${()}, command substitution (se non genera comandi), process substitution, quote removal. Questi solo per gli operandi. Può andare a capo. Si possono usare gli operatori logici !, &&, , (). <p>Operatori unari/binari non quotabili ne generaibili da command substitution:</p> <ul style="list-style-type: none"> Operazioni sui file: -e (esistenza), -d (cartelle), -f (file), -h (link), -r (leggibile), -s (size>0), -t (fd open e riferisce un terminale), -w (scrivibile), -x (eseguibile), -O (possesso effettivo utente), -G (possesso effettivo gruppo), -L (=h). Confronto date ultima modifica file: f1 -nt f2 (f1 nuovo o f2 inesistente), f1 -ot f2 (f1 vecchio o inesistente). Operatori aritmetici: -eq (==), -ne (!=), -le (<=), -lt (<), -ge (>=), -gt (>). Operatori lessicografici: ==, =, !=, i, i=, i=, i, -z (size==0), -n (size!=0). -o da vero se opzione è abilitata per la shell. <p>Versioni vecchie: [..], test ... no a capo (semmal \), -a, -o, no () . Mettere sempre spazi prima e dopo.</p>

Tilde Expansion	Descrizione
/...	Tilde espansa con il percorso assoluto della home directory dell'effective user. Valido caso con solo / e solo /.
userName/...	Tilde e userName espansi con il percorso assoluto della home directory dell'utente specificato. Valido caso con solo userName /.

Privilegi	Descrizione
chmod u+x <i>script.sh</i>	Modifica permessi file mediante formato numerico: u+x terna 0-7. Ogni numero è la somma dei valori associati ai permessi di r(4), w(2), x/s(1). Ordine: proprietario, gruppo, altri utenti. Può diventare un quartetto aggiungendo per primo l'identificatore numero dei privilegi di <i>setuid</i> , <i>setgid</i> , <i>sticky bit</i> .
chgrp ???	Modifica il gruppo di appartenenza di un file.
chown <i>newOwner</i> <i>nameFile</i>	Modifica il proprietario (e anche gruppo) di un file.
ls -al <i>nomeFile.estensione</i>	Mostra permessi, anche dei file nascosti. Interpretazione: 1°carattere tipo file (- file, d directory, c collegamento seriale, b device a blocchi), 9 caratteri successivi terzine di permessi (r read,w write,x/s execute) per proprietario, gruppo, altri utenti.
whoami	Dice all'utente corrente le sue informazioni.
sudo <i>comando</i>	fa eseguire il comando come administratore, può essere chiesta userPass. Solo utenti gruppo sudo (gestito dall'admin) possono usarlo.

Subshell	Descrizione
bash	<p>Crea una shell figlia (interattiva non di login).</p> <p>Eredita dal padre: dir. corrente, copia variabili d'ambiente. Non sono ereditate le variabili locali.</p> <p>Creata automatico per comandi raggruppati, script, processi in background. I comandi built-in sono eseguiti in shell corrente/padre.</p> <ul style="list-style-type: none"> • -c <i>script.sh</i> non interattiva. • -l -login interattiva di login.
var=val comando . source <i>script.sh</i>	<p>Scrivendo le assegnazioni prima dell'esecuzione di un comando si creano delle var. d'ambiente solo per l'imminente subshell. Non saranno ereditate da successive subshell.</p> <p>Esegue lo script nella shell corrente.</p> <p>Utile a impostare/modificare variabili shell.</p> <p>Ignorata prima riga opzionale e eseguito con interprete corrente.</p>
exit exit <i>exitStatus</i>	<p>Termina bash corrente, elimina l'ambiente e sale alla padre.</p> <p>Termina lo script restituendo un valore intero [0-255] per indicarne l'esito di terminazione. 0 indica esecuzione terminata senza errori, qualcosaltro indica un'errore. Viene restituito alla shell esecutrice.</p>
top	Mostra in tempo reale processi in esecuzione e risorse di sistema usate.
ps	Mostra i processi in esecuzione. Con l'opzione -all vedo più informazioni (PID, PPID, ecc).
set	Visualizza sia variabili locali che d'ambiente della shell corrente (anche funzioni di shell). I parametri [re]settano dei comportamenti della shell: <ul style="list-style-type: none"> • +o <i>comando</i> Disabilita il comando (tipo history). • -o <i>comando</i> Abilita il comando (tipo history). • -a Successive variabili create/modificate diverranno d'ambiente e ereditate da shell figlie. Per [ri]definire variabili locali usare export -n <i>variabile</i>. • +a Successive variabili create/modificate diverranno locali e non ereditabili da shell figlie. (default).

Uso File Descriptor	Descrizione
\$\$	Variabile con PID della shell corrente. Utile per esplofare /proc/ e fd vari processi.
exec {n}modalità file.estensione	Apre file e l'associa al fd scento dall'utente (n). Modalità: < (lettura), > (scrittura), >> (aggiungi in coda), <> (lettura e scrittura).
exec {var}modalità file.estensione	Apre file e l'associa al fd scento dall'os inserito in var.
exec {n}>&-	Chiusura di file con fd=n.
exec {var}>&-	Chiusura di file con fd contenuto in var.
program modalità file prog2 ...	Ridirezionamento input/output. Modalità: < (strin da file), > (strout sovrascrive file), >> (strout accoda a file), (output prog1 è input prog2) Per ridirezionare su uno specifico fd del programma si fa: N>, N>>, < N. Quando si omette si sottintende strin, strout, strerr. Nota: Il fine file da tastiera si fa con "Ctrl+D". Si possono fare contemporaneamente i ridirezionamenti I/O. L'ordine di specificazione non conta.
program 0/1/2& > file &0/1/2	Ridireziona lo strin, strout e strerr del programma nel file indicato sovrascrivendo o in un altro str.
program N> &M ...	Ridirezionare simultanea in file separati: prog 2> fileErr > fileOut Fa puntare lo stream di N allo stesso stream di M (N e M sono fd). Si possono fare più ridirezionamenti (fd e file, fd e fd) in simultanea. Sono eseguiti da sinistra a destra.
prog1 & prog2	Ridireziona lo stderr nello stdout di prog1 e lo passa allo strdin di prog2.
costrutto modalità file	Applica il ridirezionamento a tutti i comandi contenuti nel costrutto e alla condizione.
program << word	Word specificata è delimitatore di fine input da passare al comando. Nell'input la word deve essere a inizio di una riga con solo essa.
program <<< word (cmd1;...)	Ridireziona in input la word. Se si quota ("...") si possono passare più dati. Comandi eseguiti in subshell con stdin/out/err condivisi e concatenati. L'exit status è quello dell'ultimo comando eseguito. Permette ridirigere più comandi simultaneamente.

Standard input e output	Descrizione
read var	Legge dallo stdin o file una sequenze di caratteri (fino all'INVIO o a capo) e la inserisce nella variabile passata. Ignora spazi e tabulazioni inizio e fine riga (amenoche si setti IFS=""). Exit status 0=lettura eseguita, >0=eof (var="") o ultima riga senza \n (var="ultimi caratteri"). Necessario controllo con #var. Parametri che considerano spazi e tabulazioni: <ul style="list-style-type: none">• -n numero Numero massimo di caratteri da leggere.• -N numero Numero esatto di caratteri da leggere. Considera \n come semplice carattero. Usa prossime righe se attuale ha caratteri insufficiente. Una read parte dalla riga precedente, se non era stata finita di leggere (fino a \n). Il parametro -u \${var} fa leggere dal file di file descriptor in var.
read var1 ...	Alle variabili viene assegnata i-esima parola della riga tranne per l'ultima variabile che riceve la stringa rimanente. Alle variabili in eccesso viene assegnato valore vuoto.

Utilities	Descrizione
head -n n file	Mostra le prime n righe del file. Default 10.
tail -n n file	Mostra le ultime n righe del file. Default 10.
sed 's/originale/nuovo/[g n];...’ file	sostituisce il testo originale (o più testi orinali con [o1, o2, ...]) con quello nuovo, solo per la prima occorrenza. Può richiedere l'opzione -r.
	<ul style="list-style-type: none"> • Con l'opzione g si applica per tutte le occorrenze in una riga oppure a "n" occorrenze. Si possono concatenare più sostituzione applicare sulla stessa riga. • ^ significa inizio linea. Va all'inizio. • \$ significa fine riga. Va alla fine. • . significa un carattere qualsiasi. .{n} significa n. caratteri qualsiasi. .* significa 0 o più caratteri qualsiasi. • [...] caratteri o insiemi di caratteri (a1-an) da sostituire. <p>backreference: In "originale" si specificano tra () stringhe riusabili in "nuovo" tramite</p>
i-esima backreference.	
cut modalità file	Estrae colonne o intervalli di caratteri dalle righe. Modalità:
	<ul style="list-style-type: none"> • -c S-D Prende i caratteri dall'indice S all'indice D (inclusi). S o D si possono omettere e si prende dall'inizio o dalla fine fino a S o D. L'indice parte da 1.
	Posso concatenare più intervalli dividendoli con ",".
	<ul style="list-style-type: none"> • -d '...' -fN Divide la stringa in parole secondo il carattere delimitatore indicato poi seleziona la parola con l'indice f-ennesimo.
cat nomeFile.estensione	Visualizza il contenuto del file.
grep stringa [file]	Filtra le righe contenenti la stringa passata (che sarà evidenziata), anche se contenuta in altre parole, dal testo che sarà successivamente scritto (termina con "Ctrl+d") o dal file passato opzionalmente.
	<ul style="list-style-type: none"> • -v Filtra righe senza parola da evidenziare.
	<ul style="list-style-type: none"> • -i Disabilità il caseSensitive.
	<ul style="list-style-type: none"> • -h o -H Disabilita la visualizzazione del nome del file dove è avvenuta la ricerca (nel caso si cerci in più file).
	Spesso usato come secondo comando di per filtrare output di altri comandi.
tee	...

Process Identifier	Descrizione
\$\$	Variabile espansa col PID (identificatore numerico univoco di processo) della shell corrente. Col raggruppamento di comandi (...; ...) viene espanso col PID della shell più esterna.
\$BASHPID	Da in ogni caso il PID della shell corrente. Comando poco portabile.
script &	Lancia processo in background. Si omette ; (& già terminatore comando). \$! ha il pid del processo lanciato in bg (anche se sganciato). Non è aggiornata se faccio bg di un processo sospeso da Z.
jobs	Mostra lista processi background e sospesi con rispettivo indice di job. Con %indiceJob si gestisce il job.
Z	Sospende processo in foreground. Lancia il segnale SIGTSTP
C	Termina processo in foreground. Lancia il segnale SIGINT.
bg	Riprende l'esecuzione di un processo sospeso ma in background. Lancia il segnale SIGCONT.
fg %n	Riprende l'esecuzione in foreground il Job specificato. Lancia il segnale SIGCONT.
kill [-valore] pid %n [-1]	Termina processso di PID o JobId indicato. Manda un segnale (interruzione software per notificare evento asincrono), default SIGTERM=15. In generale un segnale è accettato solo se proviene dall'effective user e poi viene gestito/ignorato dal processo interessato. Segnale SIGKILL=9 non può essere ignorato. -l da tutti segnali lanciabili. Con -1 si fanno terminare tutti i figli diretti della bash.
disown pid %n, ...	Sgancia jobs dalla shell. Viene sganciato ultimo job messo in bg se non si specifica nulla. <ul style="list-style-type: none"> • -r Sgancia tutti job in running. • -a Sgancia tutti job in running e suspend.
nohup script &%% %+ %	Lancia in bg e sgancia ultimo processo messo in bg. Riferisce job corrente (ultimo interrotto) in foreground o avviato in background.
%-trap "funzione/listaComandi" segnale1,...	Riferisce penultimo job interrotto in foreground o avviato in background. Azione (funzione o lista comandi) da svolge alla ricezione di certi segnali predefiniti. Funzione: nomeFunzione(){...}
wait pid %n, ...	Fa attendere la shell la terminazione del processo figlio di pid o JobId indicato (o un insieme di processi). Ha exit status l'exit status dell'unico o dell'ultimo processo terminato da attendere. Solo wait fa attendere tutti figli e da exit status 0.

Terminologia:

- **Processo:** Minima unità completa ed'autonoma d'elaborazione. Composto da più thread operanti in un contesto = spazio d'indirizzamento + tabella dei descrittori di file aperti.
- **Gruppo di processi:** Insieme variabile di processi avviati da un processo padre.
- **Terminale di controllo:** astrazione della console=video+tastiera (stdin, stdout, stderr) opzionale per un processo.
- **T.c. del gruppo di processi:** terminale controllo padre ereditato dai figli, ameno di sganciamenti volontari.
- **Sessione:** Creativa e legata a un terminale di controllo da una shell (leader sessione). sessionId=PID leader sessione. Shell prende dal terminale di controllo stdin, stdout, stderr.
Processi figli apparteranno alla sessione, ameno di distacchi, e condividono terminale di controllo.
Un terminale è t.c. per una sola sessione alla volta. La chiusura del t.c. comporta la terminazione dei processi del gruppo (SIGHUP).
- **Processo background:** Controlla terminale da cui è stato lanciato (stdin collegato e impedisce esecuzione fino alla sua fine ad'altri programmi).
Uno processo background alla volta.

- **Processo background:** Eseguito in parallelo rispetto bash madre (bash può leggere e eseguire indipendentemente). Hanno una copia fd della bash.
Terminati, ameno di sganciamento, alla chiusura del terminale della bash madre (stdin condiviso).
Più processi background alla volta.
- **Job control:** Componente che cambia stato processi da background a foreground e viceversa.
- **Jobs:** Processi in background o figli sospesi di una shell
- **Processo zombie:** Processo figlio terminato (risorse state rilasciate dall'os) di cui l'os mantiene il pcb (pid, exit status, ecc).
Del tutto eliminato quando padre fa la wait (rilascio pcb).
- **Processo orfano:** Processo figlio di cui il padre è terminato senza fare wait. Viene adottato dal processo init (PID=1) di cui farà la wait periodicamente (rilascio pcb).

Vari	Descrizione
./ comando	Esegue comando presente nella directory corrente (percorso relativo). Alternativa è inserire il percorso relativo o aggiungere il percorso assoluto alla variabile PATH.
strace comando	Dice la sistem-call usata.
clear	Pulisce la CLI. Non modifica variabili create.
which comando	Cerca in PATH il comando e se lo trova mostra il path in cui si trova.
lsmod	Elenca tutti i moduli attivi.
modinfo nomeModulo	Dice le informazioni sul modulo specificato.
sudo modprobe nomeModulo	Carica il modulo specificato.
history	Visualizza comandi, numerati, precedentemente eseguiti, anche da shell precedentemente chiuse. Con !NUMERO lancia il comando corrispondente nell'elenco di history. Con !STRINGA lancia il comando più recente che corrisponde alla stringa.
find file	Trova percorsi di file in sotto alberi della memoria. <ul style="list-style-type: none"> • -type d Trova solo directory. • -tipe f Trova solo file. • -maxdepth n Limita la profondità di ricerca al numero di livelli indicato. • -mindepth Indica il livello minimo di ricerca. • -name "..." Definisce un vincolo sul nome del file da trovare. • -iname Disabilita il caseSensitive. • -exec ... "..." \; Istruzioni da fare quando viene trovato un elemento. L'output di find viene messo al posto di ".
wc	Dice il testo passatogli il numero di righe, parole e caratteri.

Directory /proc : info sui processi, con una dir. per ogni processo attivo, create e cancellate continuamente.
 Directory sulla RAM /proc/ : contiene i processi in esecuzione e nella sottodirectory fd i file descriptor aperti.

Costrutti controllo flusso	Descrizione
for varName in elencoParole ; do listCommand ; done	Dopo il for variabile è usabile.
for ((exp1 ; exp2 ; exp3)) ; do listCommand ; done	Le exp sono espressioni valutate aritmeticamente.
if listA ; then listB ; [elif listC ; then listD ; ...] ... [else listZ ;] fi	...
while list ; do list ; done	...

In tutti i costrutti l'exit value è o quello della lista do comandi o 0 se nessun comando viene eseguito.

Espressioni condizionate su file o variabile: [condizione di un file]. Valutazione di un'espressione matematica applicata a variabili d'ambiente: ((istruzioni con espressione))

2 Crittografia

Algoritmo pubblico/noto, robusto e chiavi segrete (o note in parte) di varie dimensioni.

- Codificare (E): $testoOriginale + chiaveCodifica \xrightarrow{codifica} testoCodificato$.
- Decodificare (D): $testoCodificato + chiaveDecodifica \xrightarrow{decodifica} testoOriginale$.

Impossibile ottenere testo originale dal testo cifrato senza conoscere la chiave.

2.1 Crittografia Simmetrica (chiave segreta)

Stessa chiave K per codificare e decodificare per A e B .

+Veloce, +Efficente, -distribuzione chiavi fase riscossa, -tante chiavi ($n^*(n-1)/2$).

$$A_K \xrightarrow{testo} E_K \xrightarrow{E_K(testo)} D_K \xrightarrow{testo} B_K$$

Algoritmo noto a tutti, chiave nota solo a A e B .

- SI: segretezza, autenticazione, integrità
- NO: Non repudiabilità

Adottato da Des, Triple-DES, AES, ecc.

2.2 Crittografia Asimmetrica (chiave pubblica)

Una chiave pubblica/nota (K^+) e una chiave privata/segreta (K^-) sia per A che per B **correlate**¹. A e B non codividono chiavi segrete.

Due chiavi private-pubbliche (correlate) criptano e decriptano in modo reciproco. La chiave privata è incalcolabile dalla chiave pubblica.

+Sicurezza (non scambio completo chiavi), -Lento, -azzenza chiavi pubbliche proprietà.

Configurazioni:

- A sa a chi spedisce ma B non sa chi gli scrive.

$$A_{K_A^-}^{K_A^+} \xrightarrow{testo} E(K_B^+) \xrightarrow{K_B^+(testo)} D(K_B^-) \xrightarrow{testo} B_{K_B^-}^{K_B^+}$$

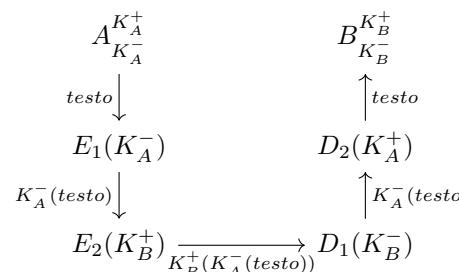
SI: segretezza.

- A non sa chi capisce cosa scrive ma B sa chi scrive.

$$A_{K_A^-}^{K_A^+} \xrightarrow{testo} E(K_A^-) \xrightarrow{K_A^-(testo)} D(K_A^+) \xrightarrow{testo} B_{K_B^-}^{K_B^+}$$

SI: Autenticazione, Integrità, Non repudiabilità.

- A sa chi capisce cosa scrive e B sa chi scrive.



SI: Segretezza, Autenticazione, Integrità, Non repudiabilità.

Adottato da RSA, ecc.

¹Un testo cifrato con una chiave può essere decriptato solo dalla chiave a cui è correlata (legata).

2.2.1 Funzioni Hash Crittografiche

Una **Funzione Hash crittografiche** ($MD()$) (one-way hash, funzioni digest) prende in input un messaggio (m) lungo a piacere e da in output un digest (stringa) a lunghezza fissa ($MD(m)$).

Il digest non è reversibile, ossia non esiste $MD(x) = MD(y)$ oppure dato $y = MD(x), x$ è indeterminabile.

Più due m sono simili più i digest sono diversi. Più due m sono diversi non è detto che i digest siano molto diversi.

Le hash non sono decodificabili, non servono chiavi di cifratura. Le funzioni di codifica/decodifica non restituiscono output a lunghezza fissa.

Hash è diverso per quanto simili dal checksum (perchè è reversibile).

Funzioni hash: MD5, SHA-1/2(x, 256, 512, ecc)/3, ecc.

2.3 MAC e Firma digitale

MAC (Message Authentication Code) è una tecnica, veloce, di autenticazione parziale dell'origine di un messaggio. Inoltre garantisce l'integrità del messaggio.

MAC: Si attua combinando crittografia simmetrica e funzioni Hash crittografico. Attori devono conoscere la chiave segreta. Assente autenticazione di chi spedisce (potrebbe essere l'altro o se stesso). SI: Integrità, autenticazione.

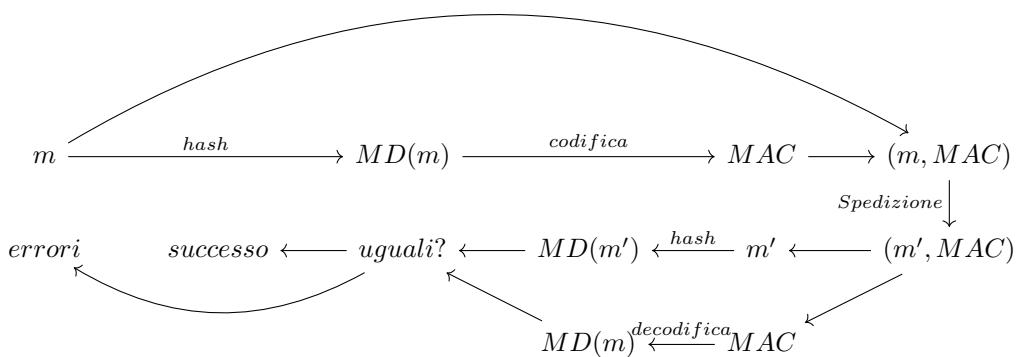
Firma Digitale: Tecnica di MAC avanzata. Si attua combinando crittografia asimmetrica e funzioni Hash crittografico. Mit. deve avere chiavi assimetriche. Chiunque può leggere e verificare l'integrità. SI: Integrità, Autenticazione, Non repudiabilità.

Spedizione:

1. Applico Funzione hash crittografico a m ottenendo $MD(m)$.
2. Codifico il digest simmetricamente o asimmetricamente (con la chiave privata del mittente) ottenendo il MAC.
3. Concatenazione MAC al m .
4. Spedizione (m, MAC) che può modificare m in (m', MAC) .

Ricezione:

1. Separazione di (m', MAC) .
2. Decodifica simmetrica o asimmetrica (usa chiave pubblica mittente) del MAC ottenendo il digest ($MD(m)$). Terminazione improvvisa se decodifica non da successo. Implica che mittente non è quello atteso.
3. Applico Funzione hash crittografico a m' ottenendo $MD(m')$.
4. Confronto i due digest. Se sono uguali m' è l'originale spedito dal mittente dichiarato.



2.4 GPG e PGP

GPG meccanismo di firma digitale gratuito basato su PGP proprietario. Garantisce autenticità e integrità di un file/package.

Il **maintainer**² della risorsa possiede chiavi asimmetriche e per ogni risorsa da pubblicare crea la firma digitale e la distribuisce con la risorsa. Oggi firmato solo file indice di risorse (Release.gpg) che ha versione e checksum (digest) di ogni risorsa.

L'utente, scarica se non l'ha la chiave pubblica, scarica il package+firma cerifica firma con la chiave pubblica del maintainer.

Le chiavi pubbliche si possono trovare di default nell'OS o si scaricano da canali ufficiali verificando a modo.

²Qualcuno che distribuisce, assicura il funzionamento e aggiornamento di una risorsa online.

3 Programmazione Concorrente

Inclusioni necessarie:

- `#include <sys/types.h>` Definire tipi di dato speciali usati nelle chiamate di sistema.
- `#include <unistd.h>` Include funzioni e costanti del sistema operativo Linux/Unix.

Multi-processo	Descrizione
fork()	Crea un processo figlio. Condivide codice successivo alla fork e possiede una copia dei dati. Restituisce il pid del figlio al padre ($PID_F > 0$) e 0 al figlio ($PID_F = 0$) o un codice d'errore ($\neq 0$).
exit(0)	Termina un processo restituendo lo stato indicato come parametro (0 stato successo).
wait(NULL)	Se padre termina prima del figlio non si possono liberare le risorse. Fa attendere al processo la terminazione del processo figlio. Restituisce il pid del processo terminato.
wait(pidProcesso)	Fa attendere al processo corrente uno specifico processo.
waitpid(pidProcesso, &status, statoAtteso)	Fa aspettare un thread specifico con uno stato specifico.
exec	Sostituisce codice e dati a un processo. Non crea processi figlio.

Un processo possiede: Il proprio PID (gestito dall'os), il PID del processo figlio o 0 e il pid del processo "iziale" (gestito da descrittore di file).

Struttura base programma multi-processo:

```
int main() {
    pid_t pid;

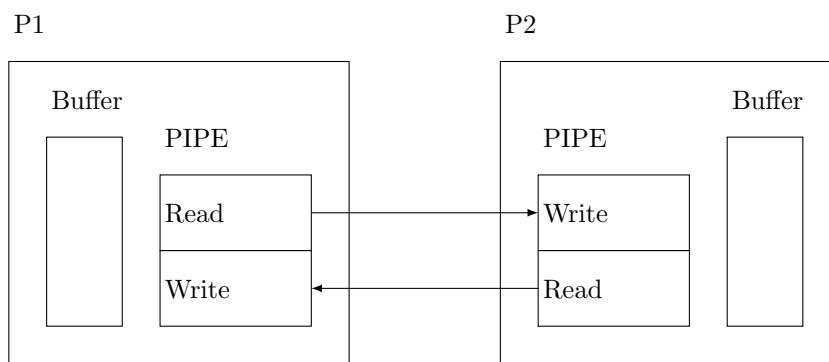
    pid = fork();

    if (pid < 0) { "gestione errore" }
    else if (pid == 0) { "processo figlio" }
    else { "processo padre" }
}
```

Ogni processo tiene referenza di un unico figlio, anche se ne può creare diversi. Quindi dopo ogni fork è buona cosa separare i flussi dei due processi.

PIPE	Descrizione
pipe(varPipe[2] : int) : int	Crea una pipe unidirezionale. Su varPipe[0] si leggerà. Su varPipe[1] si scriverà. Restituisce -1 in caso di errore, 0 se creazione avviene con successo.
close(varPipe[0 1])	Chiude una estremità della pipe.
read(varPipe[0], buffer, bufferSize)	Blocca esecuzione in attesa di dati da leggere.
strcpy(buffer, "...")	Prepara il buffer con il messaggio da inviare.
write(varPipe[1], buffer, sizeBuffer+1)	Scrive nella pipe.

Permette di comunicare fra processi correlati usando system-call e i descrittori di file. Il collegamento esiste fino a eliminazione esplicita o del processo.



Ogni processo ha un buffer di caratteri e una pipe (array di due celle) per scrivere e leggere con l'altro processo i dati contenuti nel buffer.

Nota: I processi sono visti come file, per questo le operazioni si chiamano come quelle dei file.

Multi-thread	Descrizione
nomeFunzioneThread(arg : void*) : void*	Funzione assegnata da eseguire a un thread. Necessita questa firma specifica per accettare e restituire qualsiasi tipo di dato. Serve eseguire un cast esplicito.
pthread_create(&varThread, &pthreadAttribut, tFunction, &args)	Crea un nuovo thread dentro al processo corrente. I parametri sono: <ol style="list-style-type: none"> 1. Variabile tipo thread. 2. Puntatore a struttura di attributi del thread. Default è NULL. 3. Funzione che sarà eseguita dal thread. 4. Puntatore a struttura contenente parametri usati dalla funzione.
pthread_join(&varThread, NULL)	Fa attendere processo la fine del thread indicato.

Struttura base programma multi-processo:

```
void *tFunction(void *args) {...}
int main() {
    pthread_t thread;
    ... args = ...;

    pthread_create(&thread, NULL, tFunction, &args);
}
```

Nota: La creazione di un processo è più lenta della creazione di un thread perchè nella prima bisogna creare un intero file descriptor, mentre nella seconda parziale.

3.1 SJF

Calcolo approssimato CPU Bust: $T_{n+1} = \alpha t_n + (1 - \alpha)T_n$.

- t_m tempo n-esimo CPU burst. Storia recente.
- T_n previsione prevista. Storia passata.
- α peso storia recente e passata.

Calcolo Media esponensiale: $T_{n+1} = \sum_{j=0}^n \alpha(1 - \alpha)^j t_{n-j} + (1 - \alpha)^{n+1}T_0$.

3.2 Produttore e consumatore

$[producer] \xrightarrow{\text{genera/trasferisce}} < \text{variable} > \xleftarrow{\text{consumo/preleva}} [consumer]$

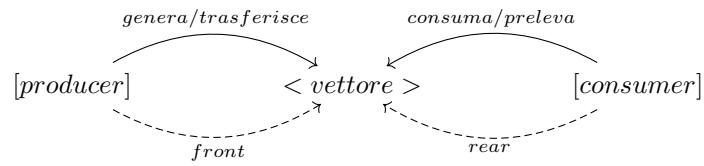
```
shared Object buffer;
Semaphore empty =
  new Semaphore(1);
Semaphore full =
  new Semaphore(0);

cobegin
  Producer
  // 
  Consumer
  coend

process Producer {
  while (true) {
    Object val = produce();
    empty.P();
    buffer = val;
    full.V();
  }
}

process Consumer {
  while (true) {
    full.P();
    Object val = buffer;
    empty.V();
    consume(val);
  }
}
```

3.3 Buffer limitato



```
Object buffer[SIZE];
int front = 0;
int rear = 0;
Semaphore empty =
    new Semaphore(SIZE);
Semaphore full =
    new Semaphore(0);

process Producer {
    while (true) {
        Object val = produce();
        empty.P();
        buf[front] = val;
        front = (front + 1) % SIZE;
        full.V();
    }
}

process Consumer {
    while (true) {
        full.P();
        Object val = buf[rear];
        rear = (rear + 1) % SIZE;
        empty.V();
        consume(val);
    }
}
```

3.4 Filosofi orientali a cena

pensa $\xrightarrow{\text{-----}} [\text{Filosofo}] \xrightarrow{\text{mangia}} <\text{chopsticks}>$

```
Semaphore chopsticks =
{ new Semaphore(1), ..., new Semaphore(1) };

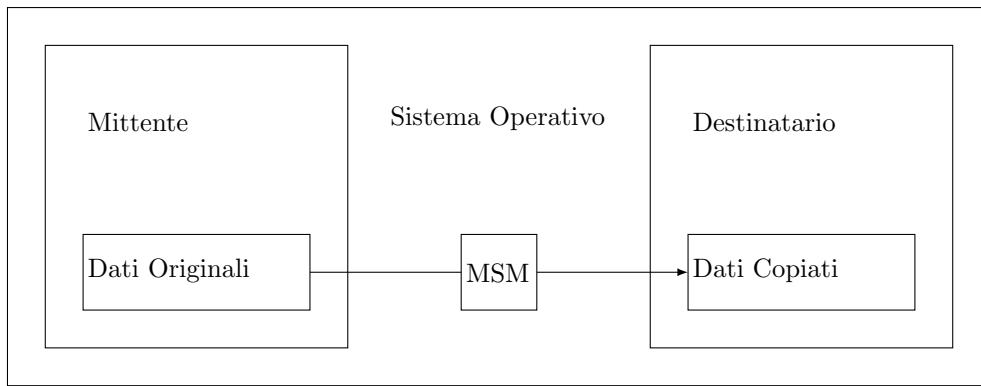
process Philo[i] { /* i = 0...4 */
    while (true) {
        think
        chopstick[i].P();
        chopstick[(i+1)%5].P();
        eat
        chopstick[i].V();
        chopstick[(i+1)%5].V();
    }
}
```

Le battecche sono un vetore lungo 5 (0...4) e i filosofi accedono alle battecche i e i+1 in %5.

Rischio di deadlock!!! Esistono varie soluzioni, avere un filosofo mancino è la più semplice:

```
process Philo[0] {
    while (true) {
        think
        chopstick[1].P();
        chopstick[0].P();
        eat
        chopstick[1].V();
        chopstick[0].V();
    }
}
```

3.5 Message Passing



Legenda: p=mittente, m=messaggio, q=destinatario.

Sincrono:

- Mittente attende l'ACK (Acknowledgement) del destinatario.
`ssend(m, q)`
- Destinatario attende la spedizione di m da p o da un qualsiasi mittente (*). Poi manda l'ACK.
`m=sreceive(p|*)`

Asincrono:

- Mittente non attende l'ACK del destinatario.
`asend(m, q)`
- Destinatario attende la spedizione di m da p o da un qualsiasi mittente (*). Non manda l'ACK.
`m = areceive(p|*)`

Completamente asincrono:

- Mittente non attende l'ACK del destinatario.
`asend(m, q)`
- Destinatario non attende la spedizione di m da p o da un qualsiasi mittente (*). Non manda l'ACK.
`m = nb-receive(p|*)`
Se non si riceve nulla restituisce `null`.

Nella pratica: lo scambio di messaggi avviene tra canali di comunicazioni su cui mandare e ricevere. L'istruzione `replay(Thoth)` sblocca il mittente (e non la receive).

3.6 Concorrenza in C

Usata la librerie POSIX **semaphore.h** (API POSIX con semafori, lock mutex e variabili condizionali).

Tipi di semaforo:

- Con nome (**named**) utile a sincronizzare processi non correlati.
- Senza nome (**unnamed**).

Funzioni semafori	Descrizione
<code>sem_t * <variabile></code>	Definisce una variabile di tipo puntatore a struttura Semaforo.
<code>sem_ini(&<varSem>, 0/altro, ¡valoreIniziale¡)</code>	Crea un semaforo unnamed inizializzato al valore passato e lo assegna alla variabile d'indirizzo indicata. Secondo parametro a 0 semaforo condiviso tra thread stesso processo, a ≠ 0 condiviso tra processi.
<code>sem_open("nomeSem", 0_CREAT,0666, ¡valoreIniziale¡)</code>	Crea e restituisce un semaforo named in R/W (3° parametro) inizializzato al valore passato.
<code>sem_wait(&varSem)</code>	Esegue l'operazione P (decrementa).
<code>sem_post(&varSem)</code>	Esegue l'operazione V (incrementa).
<code>sem_destroy(&varSem)</code>	Distrugge un semaforo.

Le CS saranno contenute tra un wait e un post.

4 Esercizi Scheduling

Procedura risolutiva di un esercizio di scheduling data la **durata del quanto di tempo** e una tabella dei processi del tipo:

Processi	Tempo di Arrivo	Tempo d'Esecuzione
...

Passo 1

Fare una tabella di scheduling come la seguente:

Ready Queue	
Running	
Quanto d'Inizio/Fine	
Tempo	0 1 ... n
T.R. P1	
...	
T.R. PN	

Spiegazione delle righe della tabella:

1. *Ready Queue* specifica per ogni quando i processi pronti per essere eseguiti, tipicamente è FIFO.
2. *Running* indica per ogni quanto di tempo il processo in esecuzione.
3. *Quanto d'Inizio/Fine* evidenzia i quanti d'arrivo (A) e di termine (F) dei processi.
4. *Tempo* sono i quanti del processore. Ogni colonna è un quanto.
5. *Righe T.R.* tempo d'esecuzione rimante per ogni processo a ogni quanto di tempo dalla sua partenza.

Passo 2

Per rispondere alle statistiche richieste fare una tabella come la seguente:

Processi	T. Turnaround	Intervalli di Ready	T. Attesa
...	...	[x1-x2],
Medie:

Spiegazione delle colonne della tabella:

1. *Turnaround* = T. fine - T. arrivo.
2. *Intervalli di Ready* sono i quanti in cui il processo è stato nella coda di ready (dal quanto in cui vi è entrato al quanto in cui vi è uscito).
3. *T. Attesa* somma degli intervalli di ready.

5 File Descriptors

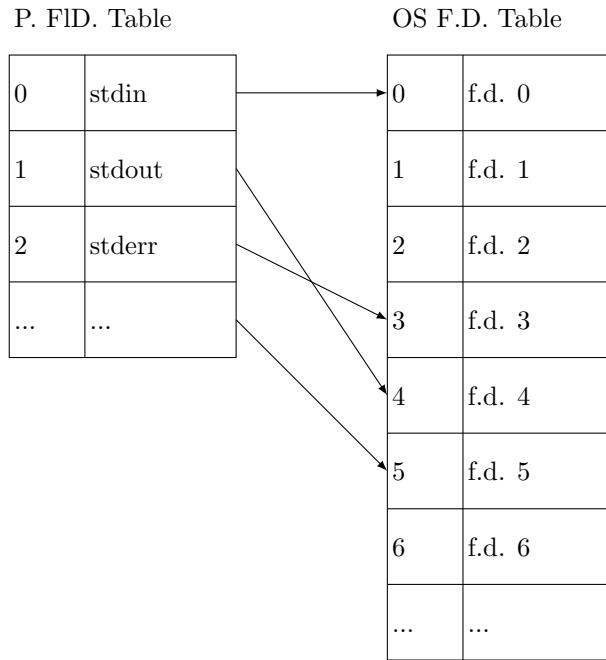
Il file descriptor è un'astrazione (integer, inizio buffer) dell'os, e quindi multi linguaggio, per permettere l'accesso ai file.

Ogni processo ha la **file descriptor table** di record indiretti delle informazioni (file descriptor) sui file aperti dal processo stesso. I record sono indiretti perché puntano ai record della **tabella di sistema**. La tabella di sistema contiene file descriptor dei file attualmente aperti.

Un processo/shell figlia eredita una copia della f.d. table, successivamente modificabile. Padre e figlio si devono sincronizzare sull'accesso ai file. Ciò permette un modo di comunicazione tra i processi.

Rindizionamenti:

- **Processi figlio:** Padre può cambiare le associazioni fd/stream passate al figlio.
- **Auto-ridirezionamento:** fd viene associato a stream diverso.



In POSIX per ogni processo i file descriptor standard sono: stdin=0, stdout=1, stderr=2.

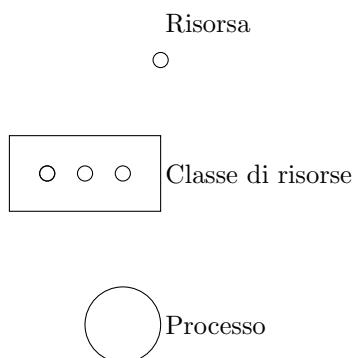
Ricorda che `stdin` è lo stream input da tastiera e `stdout` e `stderr` sono gli stream a video dell'output e dei messaggi d'errore.

Nota: Processi diversi possono avere file descriptor diversi, ma con stesso valore, e che referenziano file diversi.

In C per scrivere si usa `fprintf(stdout/stderr, "...")` [, parametri] e per leggere si usa `fgets(buffer, size, stdin)`, per il fine file usare `feof(stdin)`.

6 Risorse

6.1 Grafo di Holt Generale (classi e processi)

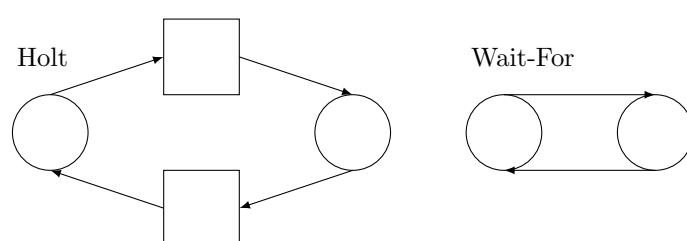


Per gli archi si può segnare la molteplicità, e nelle classi il numero di risorse non assegnate.

6.2 Detaction and recovery - Caaso 1

Teorema: Siano le risorse ad'accesso mutualmente esclusivo, seriali e non prerilasciabili. Con una risorsa per classe si ha deadlock \iff Holt contiene un ciclo (attesa circolare).

Dimostrazione: In un grafo di Holt si ha attesa circolare se si ha attesa circolare nella rispettiva variante di grafo Wait-For (elimina le risorse collassando gli archi appropriati).



6.3 Detaction and recovery - Caaso 2

Teorema: Siano le risorse ad'accesso mutualmente esclusivo, seriali e non prerilasciabili. Con più risorse per classe si ha deadlock \iff Holt non è completamente riducibile (eliminazione tutti archi).

6.4 Detaction and recovery - Knot

Teorema: Siano le risorse ad'accesso mutualmente esclusivo, seriali e non prerilasciabili. Con una richiesta sospesa per processo si ha deadlock \iff esiste un knot.

6.5 Stato SAFE - algoritmo del banchiere

Sia s una permutazione dei valori $1, \dots, N$ e $s(i)$ l'i-esima posizione nella sequenza. Si calcola il vettore **avail** così:

1. $\text{avail}[1] = SC$
2. $\text{avail}[1+j] = \text{avail}[j] + p_{s(j)}$, con $i=1, \dots, N-1$

Uno stato del sistema è safe se vale: $n_{s(j)} \leq \text{avail}[j]$, con $j=1, \dots, N$.

Con il banchiere a singola valuta basta ordinare in modo crescente gli n_i per assicurare lo stato SAFE.

Nel caso multi valuta si aggiunge il pedice k della valuta.

Con il banchiere multi valuta ogni valuta ha un suo ordine.

7 Gestione Pacchetti in Linux

7.1 Concetti chiave

- **Package (.deb)**: archivio compresso di file descrivono programma e metadati del package.
- **Dipendenze**: Librerie necessarie funzionamento programma.
- **Repository**: Collezioni locali o remote di package in server centralizzati.
- **Database locale di package**: Elenco locale dei metadati di package nei repository.

7.2 Installazione Package

Interfaccia a CLI per download-installazione (risolve dipendenze e gestisce fonti), rimozione, aggiornamento, gestione di package. Usa **dpkg** per l'installazione vera e propria (disassembla package e installa in directory giuste) e **apt-cache** per la ricerca (usabili anche dall'utente).

Assente di descrizione esecuzione (ideale per script).

apt-get

apt fornisce una descrizione testuale della procedura eseguita (user friendly).

Comandi apt-get	Descrizione
update	Aggiorna database locale di package. Da eseguire per primo.
upgrade	Installa le nuove versioni dei package già installati.
install	Installa un package nuovo e le dipendenze.
remove	Rimuove package lasciando file configurazione.
purge	Rimuove package e file configurazione.
autoremove	Rimuove package, non più necessari, autoinstallati soddisfare dipendenze altri package.
dist-upgrade	Aggiorna la distribuzione (package e dipendenze).
clean	Cancella package dalla cache locale.

Formato generico: **sudo apt-get "comando" "packageOpzionale"**

Procedura Installazione Package:

1. **sudo apt-get update** Aggiorna l'indice/database locale scaricando l'elenco aggiornato dei package e versioni dai repository.
2. **apt-get intall "package"** Installa il package cercandolo nel database locale e controllando le dipendenze.

7.2.1 Posizione Repository

I database locali di package sono contenuti in: `/etc/apt/sources.list` (principale), `/etc/apt/sources.list.d/` (aggiunte repository individuali).

Formato one-line: `deb [opzioni] URI distribuzione comp1 comp2 ...`

- **Tipo:** Indica il tipo d'archivio.
`deb` indica package binari precompilati.
`deb-src` indica package di sorgenti.
- **Opzioni:** La firma GPG si attua col campo dedicato che accettà il **keyring** con la public-key del maintainer.
`signed-by="..."`
- **URI:** Indirizzo del repository.
- **Distribuzione:** Nome in codice della versione del OS.
- **Componenti:** Definiscono il tipo di licenza (main, restricted, universe, multiverse).

Caratteristiche: chiarezza, leggibilità, facile da gestire e sicurezza esplicità.
C'è anche un formato deb822 più leggibile.

Directory public-key: `/usr/share/keyrings/` (key di sistema), `/etc/apt/keyrings/` (key d'utente).

Il `keyrings`, `sources.list`, `sources.list.d/` sono editabili con editor con privilegio sudo o GUI specifiche.
Aggiunta Manuale:

1. Verificare esistenza directory, scarica GPG-key (sopprime output e reindirizza allo stdout), comprimerla (ASCII in binario .gpg) e salvataggio nel keyring.

```
sudo mkdir -p /etc/apt/keyrings  
wget -qO- URI | sudo gpg --dearmor -o directory.gpg
```

2. Aggiungere riferimento one-line con signed-by del repository alla directory.

```
echo "FormatoOneLine" | sudo tee directory.list
```

3. Aggiornamento e installazione: `sudo apt update`, `sudo apt install nomePackage`.