



Sicurezza delle Reti

*Corso di Laurea in Ingegneria Informatica
I livello, III anno, II semestre*

Prof. Stefano Bregni

Politecnico di Milano - DEIB

Tel. 02 2399.3503 – Email: <stefano.bregni@polimi.it>

Stefano Bregni

Contenuti principali

- Introduzione alla sicurezza nelle reti di comunicazione (Internet)
- Crittografia
 - ◆ introduzione alle basi teoriche della crittografia e alla teoria dei numeri (matematica dei numeri interi o matematica discreta)
 - ◆ algoritmi di cifratura sia a chiave simmetrica sia a chiave pubblica
- Protocolli e sistemi per la comunicazione sicura in rete
 - ◆ metodi e protocolli di autenticazione di persone e di messaggi
 - ◆ certificati, hash e firme elettroniche
 - ◆ protocolli di scambio e instaurazione delle chiavi di cifratura
- Seminari monografici complementari tenuti da esperti dell'industria o operatori di telecomunicazioni

Programma (1)

- Introduzione alla crittografia e alle comunicazioni sicure
- Basi di teoria dei numeri (matematica discreta)
 - Nozioni di base di aritmetica modulare. Numeri primi. Operazioni modulo n : congruenze, divisioni, elevamento a potenza. Algoritmo di Euclide. Teoremi di Fermat e di Eulero. Elementi primitivi. Radici quadrate mod n .
- Cifrari a chiave simmetrica
 - Cifrari classici. Cifrari a blocchi. Cifrari a catena. Algoritmo DES. Algoritmo AES.
- Generazione di bit pseudocasuali
 - Algoritmo Blum-Blum-Shub. Successioni LFSR da registri a scorrimento retroazionati. Applicazioni ai sistemi di comunicazione (scrambling).
- Cifrari a chiave pubblica
 - Algoritmo di cifratura a chiave pubblica RSA. Test di primalità. Fattorizzazione. Logaritmo discreto. Algoritmo di cifratura a chiave pubblica di El Gamal.

Programma (2)

- Autenticazione dei messaggi: funzioni hash e firma elettronica
 - Funzioni di hash. SHA. Attacco del compleanno. Firma RSA. Firma di El Gamal.
- Protocolli di distribuzione delle chiavi
 - Distribuzione, scambio e instaurazione di chiavi simmetriche, senza e con autenticazione. Protocollo di invio chiave di Shamir-Omura. Protocollo di instaurazione della chiave di Diffie-Hellman. Protocollo station-to-station. Schema di predistribuzione delle chiavi di Blom. Protocollo wide-mouthed-frog. Protocollo di Needham e Schroeder.
- Autenticazione e infrastruttura a chiave pubblica (PKI)
 - Protocolli di autenticazione basati su Sfida e Risposta. Password monouso (OTP). Kerberos. Autorità di certificazione. Certificati.
- Protocolli e sistemi per la sicurezza di rete
 - IPsec. Firewall. Sicurezza della posta elettronica: PGP e S/MIME. SSL e TLS.



Attività Complementari

- Seminari monografici su temi vari di sicurezza delle reti tenuti da esperti dell'industria
 - Esempi di argomenti: protocolli di autenticazione, sicurezza nelle reti radiomobili, firewall, malware, attacchi e protezione dei sistemi informatici e di comunicazione.

Libri di testo e bibliografia

- Wade Trappe, Lawrence C. Washington, *Crittografia. Con elementi della teoria dei codici*. Pearson / Prentice Hall, 2a edizione, 2009
- William B. Stallings, *Network Security Essentials: Applications and Standards. 6th Edition*. Editore: Pearson, Anno edizione: 2016
- Appunti vari distribuiti a cura del docente
- Materiale degli eventuali seminari monografici
- Si consiglia di seguire le lezioni e le esercitazioni per un'ottimale comprensione di tutti gli argomenti
- Osservazioni ovvie:
 - ◆ NON si prepara un esame imparando a memoria gli svolgimenti degli esercizi assegnati agli esami precedenti
 - ◆ è meglio studiare i libri di testo e il materiale distribuito dal docente, o pagine web a caso, o riassuntini scritti da anonimi?

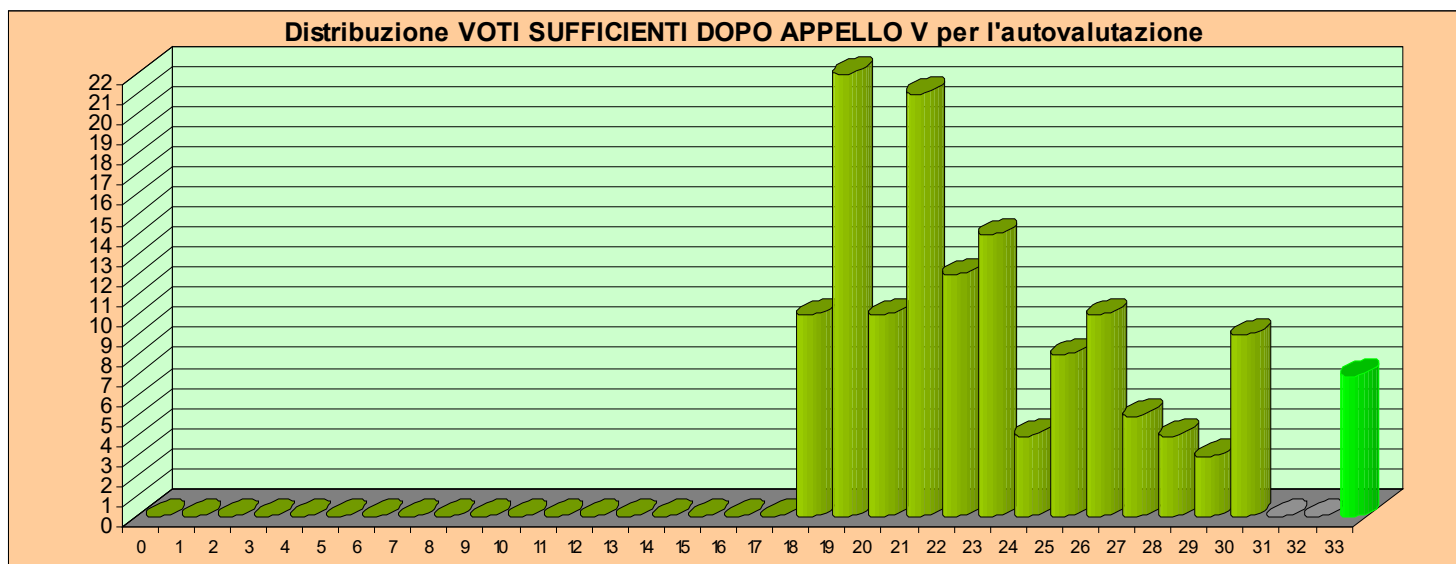
Modalità di Valutazione

- La verifica dell'apprendimento consiste in una prova scritta comprendente esercizi e domande su argomenti di teoria
- Lo studente che non si ritenga soddisfatto della votazione conseguita è ammesso agli appelli successivi per tentare di migliorare il proprio voto sino all'ultima sessione dell'A.A.
 - ◆ Consegnando la prova, si annulla automaticamente ogni voto precedentemente conseguito
- La raccolta integrale dei temi d'esame del corso è disponibile in rete
 - ◆ vastissima raccolta di esercizi di tutti i tipi
 - ◆ versione da 5 CFU (Ing. INF, dal 2017/18 a oggi)
 - ◆ versione da 10 CFU (Ing. TEL, 2012/13 - 2016/17)

Statistiche voti nel 2019-20

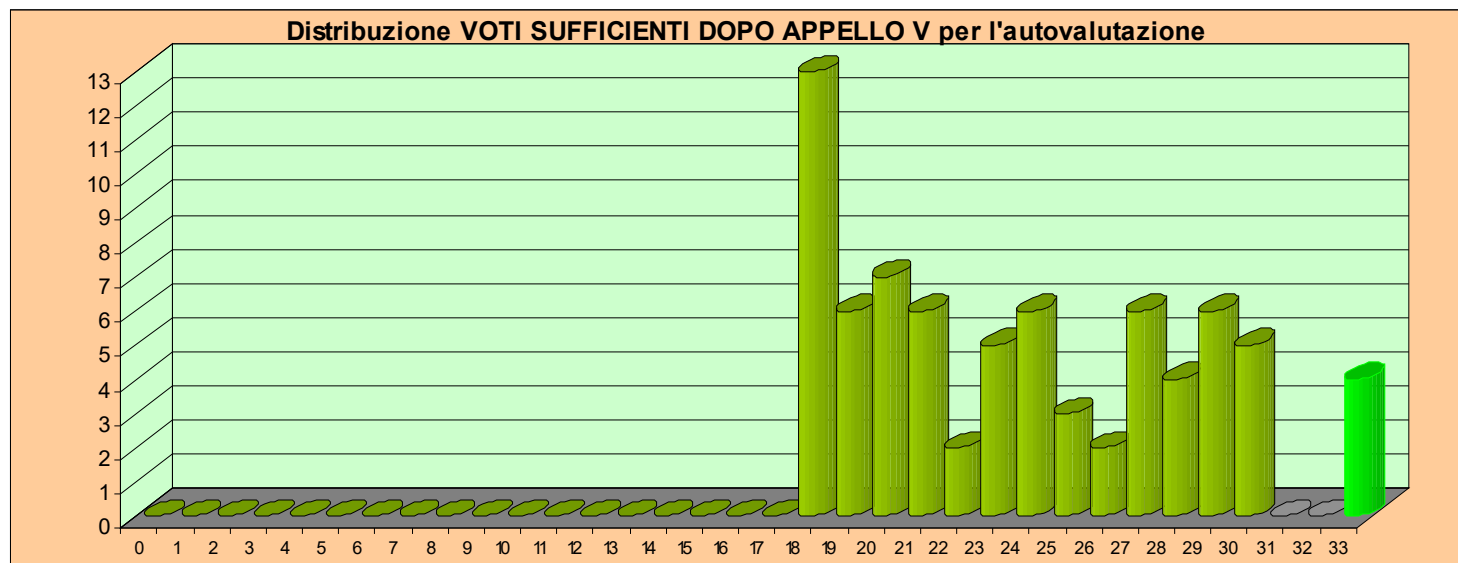
Statistiche cumulative studenti DOPO APPELLO V per l'autovalutazione

Totale iscritti	193			100%
Attivi (consegnata almeno 1 prova)	151		100%	78%
Dopo Appello V				
Con voto sufficiente ≥ 18	139	100%	92%	72%
Devono ancora superare l'esame	54			28%
Con voto >21 :	76	55%	50%	39%
Con voto >24 :	46	33%	30%	24%
Con voto >27 :	23	17%	15%	12%
Con voto >30 :	7	5%	5%	4%
Media voti	23,14			
Deviazione standard voti	4,10			



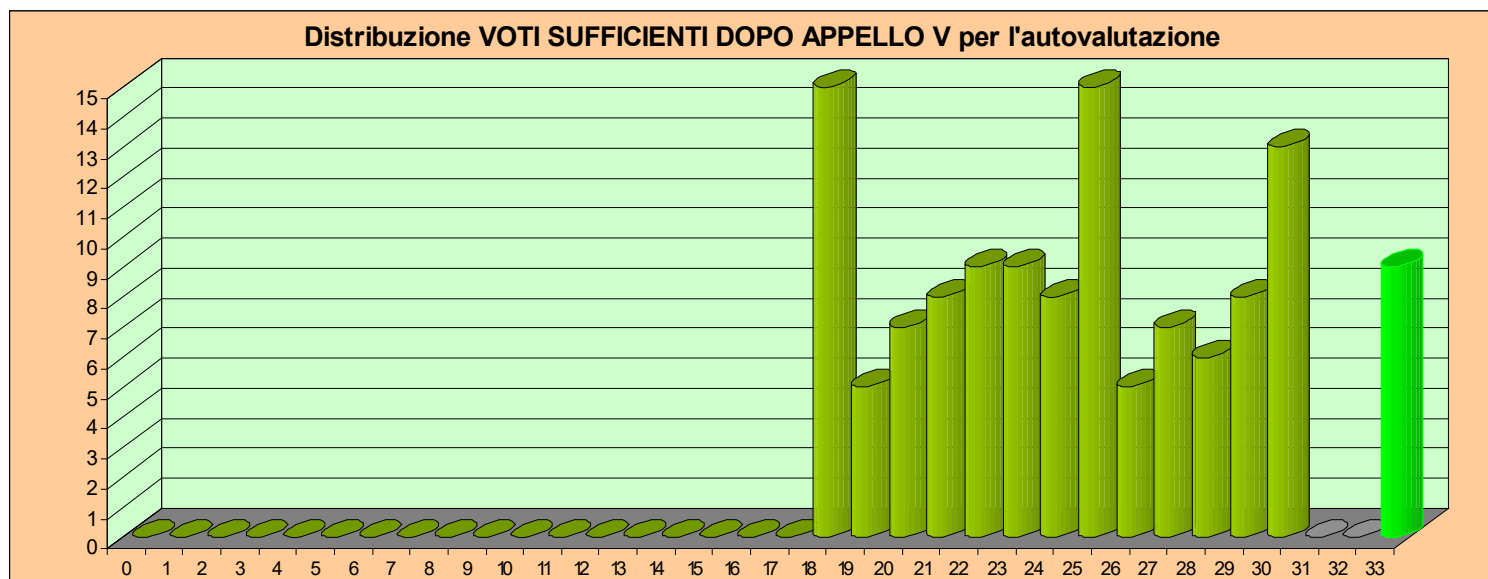
Statistiche voti nel 2020-21

Statistiche cumulative studenti DOPO APPELLO V per l'autovalutazi				
Totale iscritti	137			100%
Attivi (consegnata almeno 1 prova)	89	100%		65%
	Dopo Appello V			
Con voto sufficiente ≥ 18	75	100%	84%	55%
Devono ancora superare l'esame	62			45%
Con voto >21 :	43	57%	48%	31%
Con voto >24 :	30	40%	34%	22%
Con voto >27 :	19	25%	21%	14%
Con voto >30 :	4	5%	4%	3%
Media voti	23,65			
Deviazione standard voti	4,58			



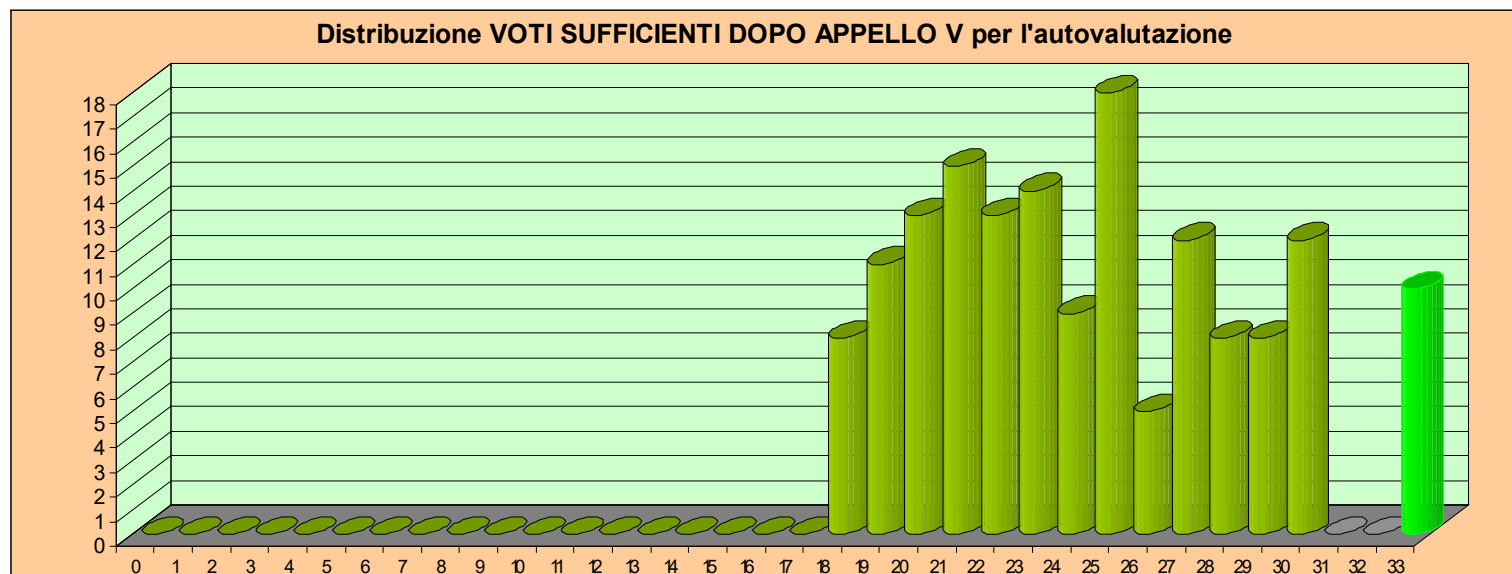
Statistiche voti nel 2021-22

Statistiche cumulative studenti DOPO APPELLO V per l'autovalutazione				
Totale iscritti	182		100%	
Attivi (consegnata almeno 1 prova)	134	100%	74%	
Dopo Appello V				
Con voto sufficiente ≥ 18	124	100%	93%	68%
Devono ancora superare l'esame	58			32%
Con voto >21 :	89	72%	66%	49%
Con voto >24 :	63	51%	47%	35%
Con voto >27 :	36	29%	27%	20%
Con voto >30 :	9	7%	7%	5%
Media voti	24,60			
Deviazione standard voti	4,44			



Statistiche voti nel 2022-23

Statistiche cumulative studenti DOPO APPELLO V per l'autovalutazi				
Totale iscritti	216		100%	
Attivi (consegnata almeno 1 prova)	164	100%	76%	
Dopo Appello V				
Con voto sufficiente ≥ 18	156	100%	95%	72%
Devono ancora superare l'esame	60			28%
Con voto >21 :	109	70%	66%	50%
Con voto >24 :	73	47%	45%	34%
Con voto >27 :	38	24%	23%	18%
Con voto >30 :	10	6%	6%	5%
Media voti	24,37			
Deviazione standard voti	4,13			



Statistiche voti nel 2023-24

Statistiche cumulative studenti DOPO APPELLO V per l'autovalutaz

<i>Totale iscritti</i>	185		100%
<i>Attivi (consegnata almeno 1 prova)</i>	140	100%	76%
Dopo Appello V			
<i>Con voto sufficiente >=18</i>	128	100%	91%
<i>Devono ancora superare l'esame</i>	57		31%
<i>Con voto >21:</i>	96	75%	69%
<i>Con voto >24:</i>	65	51%	46%
<i>Con voto >27:</i>	41	32%	29%
<i>Con voto >30:</i>	8	6%	4%
<i>Media voti</i>	24,91		
<i>Deviazione standard voti</i>	4,34		

