

Tipu di documentu	Lizzioni	Classa	2 ^{nda} SNT	Durata	1 ora	Data	05/2025
Cuntinutu	Nuzioni di sicurezza d'i cummunicazioni						
Discrizzioni	Amparera di a cudifichera simetrica è assimetrica						

A sicurezza ind'i cummunicazioni s'appoghja sempri nant'à una nuzioni assai impurtanti : a nuzioni di chjavi. A crittugraffia (κρυπτός + γράφω , "scrittura piattata") hè a scenzi chi studieghja a (s)cudifichera.

1) A cudifichera simetrica monoalfabetica : una lettara = una lettara

a) Caius Iulius Caesar

- Chì hè a chjavi quì ?

THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG
AOL XBPJR IYVDU MVE QBTWZ VCLY AOL SHGF KVN

b) Casu ghjinirali

- Chì hè a chjavi quì ?
- Quantu pussibilità c'hè ?

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
E	U	S	Y	D	G	J	B	K	W	Z	H	N	T	C	X	A	P	Q	R	M	O	V	F	I	L

- Cuntinueti di cudificà u missaghju :

D	U	M	A	N	I		S	E	R	A		A		S	E	I		O	R	I
Y	M	E																		

c) Tandu, sti 2 cudificheri sò assai debbuli...par chi ?

2) A cudifichera simetrica pulialfabetica : una lettara = parechji lettari

D'altri maneri di piattà l'infurmazioni sò stati missi in piazza à parta si da a fini di u Medievu :

"A tola d'Abulafia" - XIII^{mu} seculu, "La Cifra del Sig. Giovan Battista Bellaso" - 1553 , Vigenère - 1586

a) U squatru di Vigenère

Ogni lettara di a chjavi hè ligata à un santacruci sfarenti. Quì, a chjavi hè una parolla secreta.

Missaghju

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

- Continueti di cudificà stu missaghju, a chjavi/parolla sicreta hè "CRYPTO" :

Missaghju	D	U	M	A	N	I	S	E	R	A	A	S	E	I	O	R	I
Chjavi cù ripetizioni	C	R	Y	P	T	O	C	R	Y	P	T	O	C	R	Y	P	T
Missaghju cudificatu	F	L	K														

- Chi sò i forzi è i dibbulezzi di stu sistema ?

b) Altri cudificheri simetrici

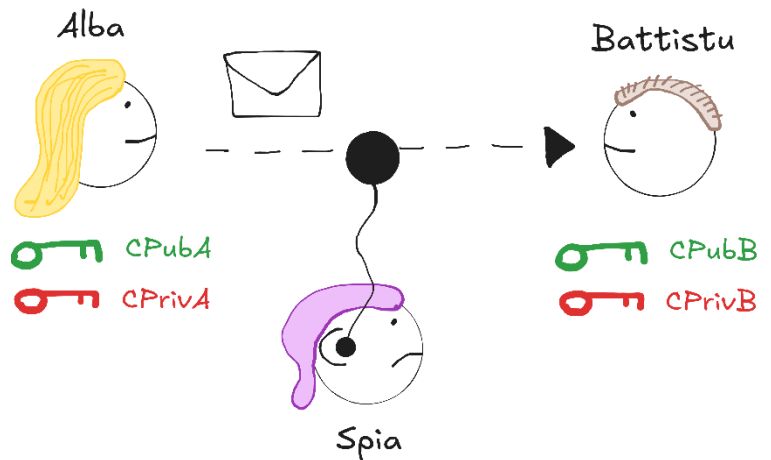
D'altri sistemi sò stati missi in piazza, ùn sò micca monoalfabetichi nemancu polialfabetichi, par asempiu DES è AES. Facini una cudifichera cù blocchi. U più cunnisciutu hè AES (*Advanced Encryption Standard*), hè quillu ch'hè adupratu oghji. Inde AES, a listessa chjavi pò cudificà è scudificà un missaghju. Studià AES saria troppu difficiuli, u so funziunamentu dumanda cunniscenzi di matematici è di programmazioni d'un livellu assai altu.

3) A cudifichera assimettrica

Parechji algoritimi sò aduprati (u più famosu hè RSA), mà i fundamenti sò sempri listessi : ogni parsona t'hà un paghju di chjavi, una hè **privata** (sicreta), ùn hè mai spartuta, è l'altra hè **pubblica**.

I dui chjavi sò ghjinerati à tempu, tandu asisiti un liamu matematicu forti trà elli, mà ùn si pò micca induvinà/calculà l'una à parta si da l'altra !

A **chjavi privata** scudifichighja i dati cudificati incu a **chjavi pubblica** (casu 1), mà dinò a **chjavi pubblica** scudifichighja i dati cudificati incu a **chjavi privata** (casu 2).



Casu 1 : Pà mandà un missaghju sicretu, Alba l'hà da cudificà incù a **chjavi pubblica** di Battistu **CPubB**. Ellu solu pudarà scudificà u missaghju incù a so **chjavi privata** **CPrivB**.

Casu 2 : Alba voli firmà un documentu elettroncu. L'hà da cudificà incù a so **chjavi privata** **CPrivA**, pà fà chi tuttu ognunu possi scudificà u documentu incu a so **chjavi pubblica** **CPubA**.

I 2 poni essa missi in ballu inseme : Alba cudifichighja dati incù **CPubB**. Dopu firma u documentu (in rialità, una parti chjamata u macinatu o "hash") incù **CPrivA**. Battistu ricevi u missaghju : pò virificà chi veni da Alba (incù **CPubA**). Dopu l'hà da scudificà incu a so **chjavi privata** **CPrivB**.

4) Crittomuneta

Nuzioni di purtafogliu (o wallet) cumpostu da :

- Un indirizzu publicu (**CPub**)
- Una parolla sicreta (**CPriv**)

Nuzioni di catena di blocchi (o blockchain) : "libru" di scambi trà wallets

Nuzioni di provi di validità : parechji parsoni ("mining") sò incaricati di virificà i movimenti (pà impidiscia i doppii spesi, è fà casu à l'ordini d'i transazzioni)

