

Informatica per le discipline umanistiche

Lezione 14 – Crittografia Simmetrica

`cristiano.longo@unict.it`



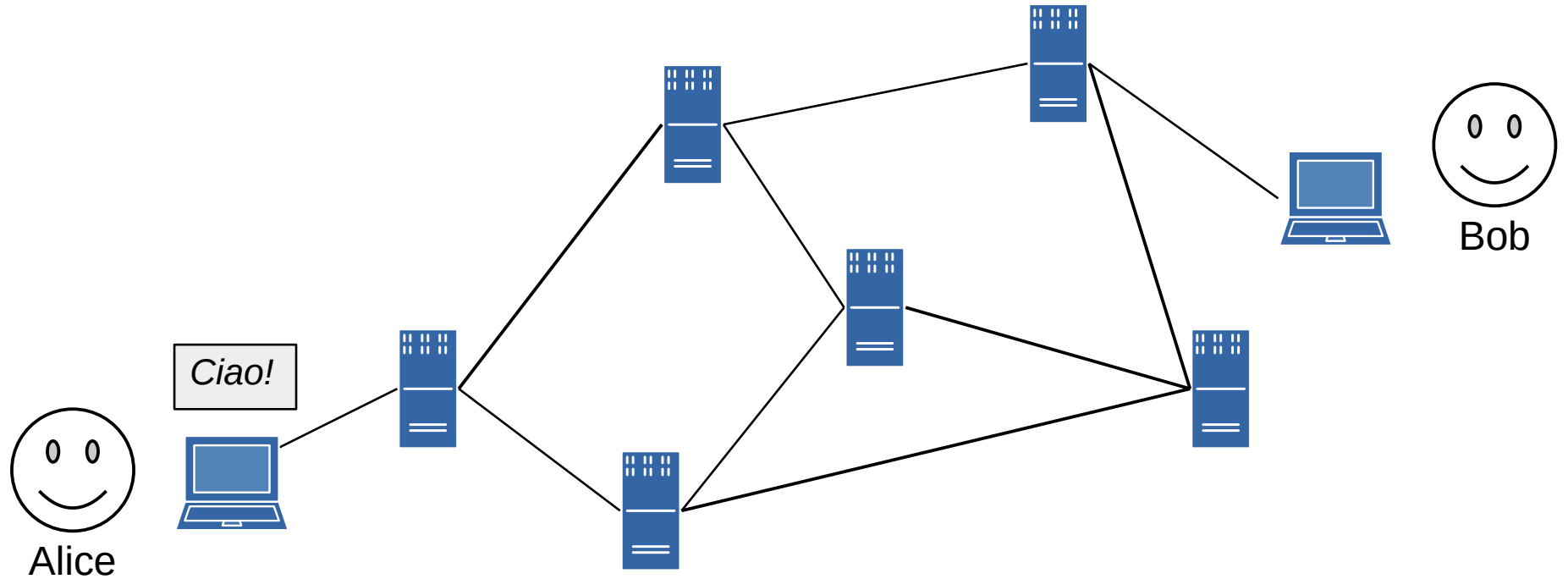
Sicurezza su Internet

Alcuni problemi di sicurezza di cui sono affette le reti di computer sono legati

- alla **privacy** (tenere *confidenziali* le proprie attività e i propri dati) e
- all'**autenticità** (essere sicuri del mittente di una comunicazione e che la comunicazione non sia stata alterata).

Privacy

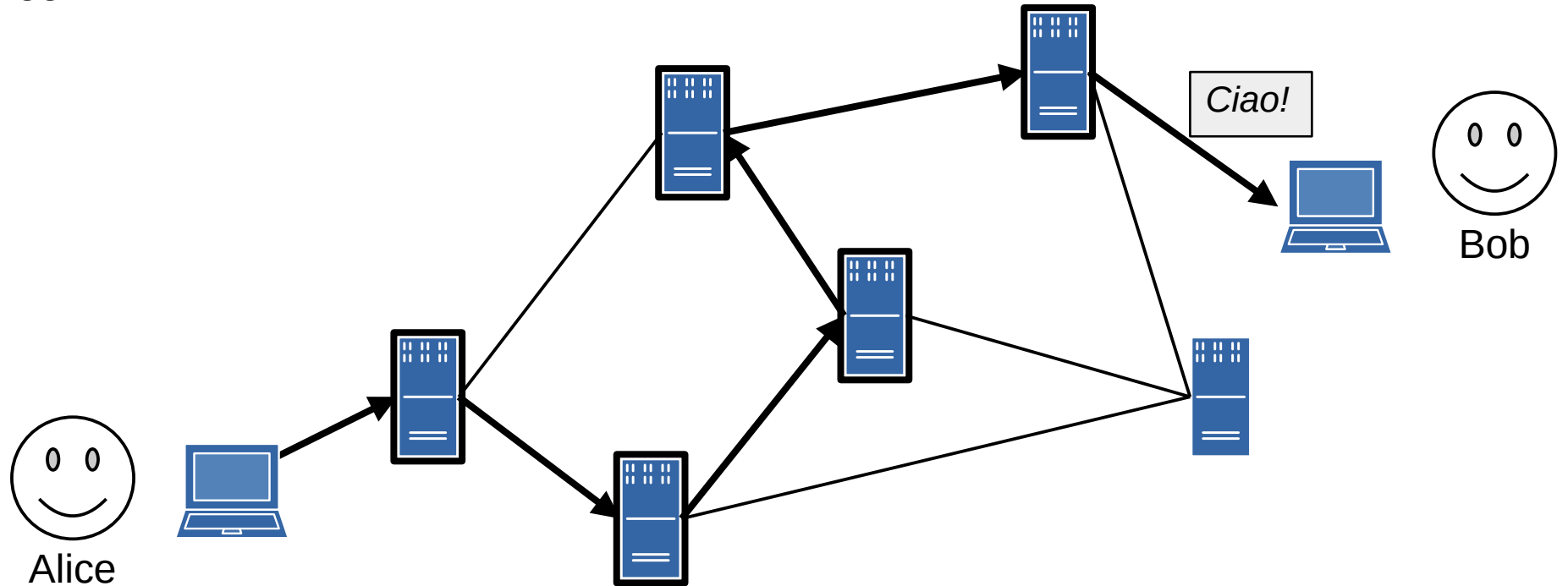
Quando inviamo un messaggio (pacchetto) ...



Privacy

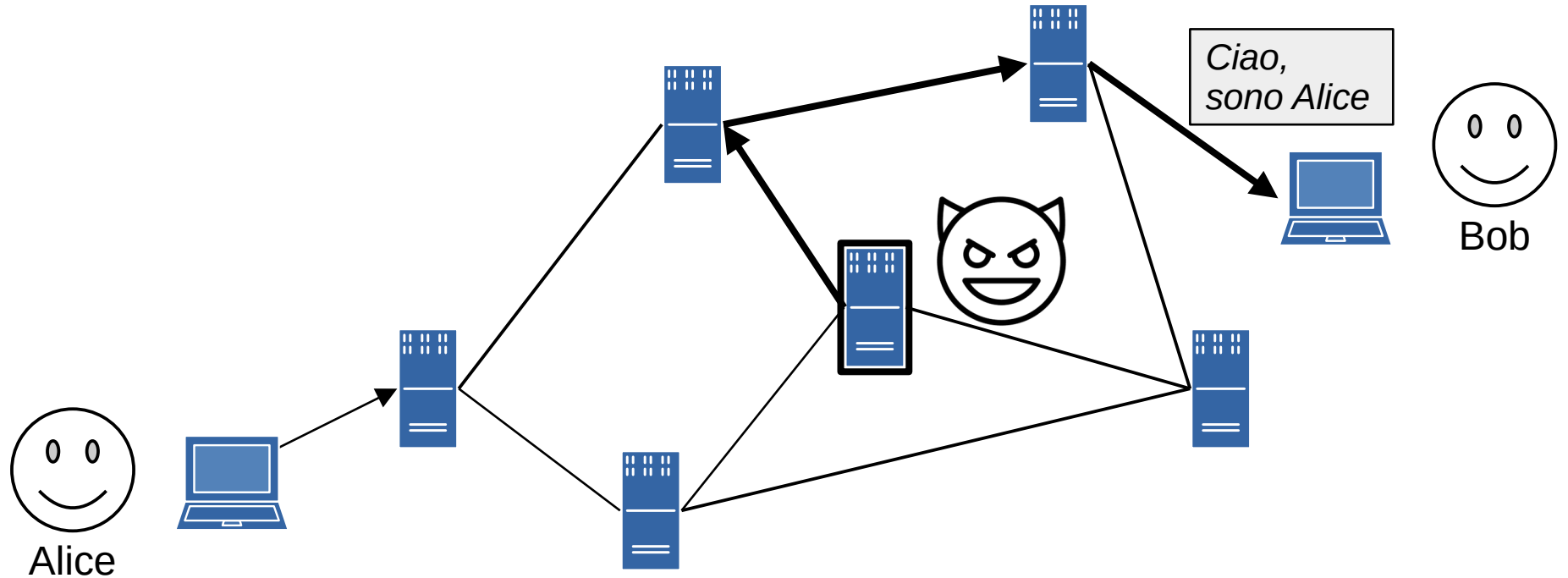
Quando inviamo un messaggio (pacchetto) molte persone possono

- leggerne il contenuto



Autenticità

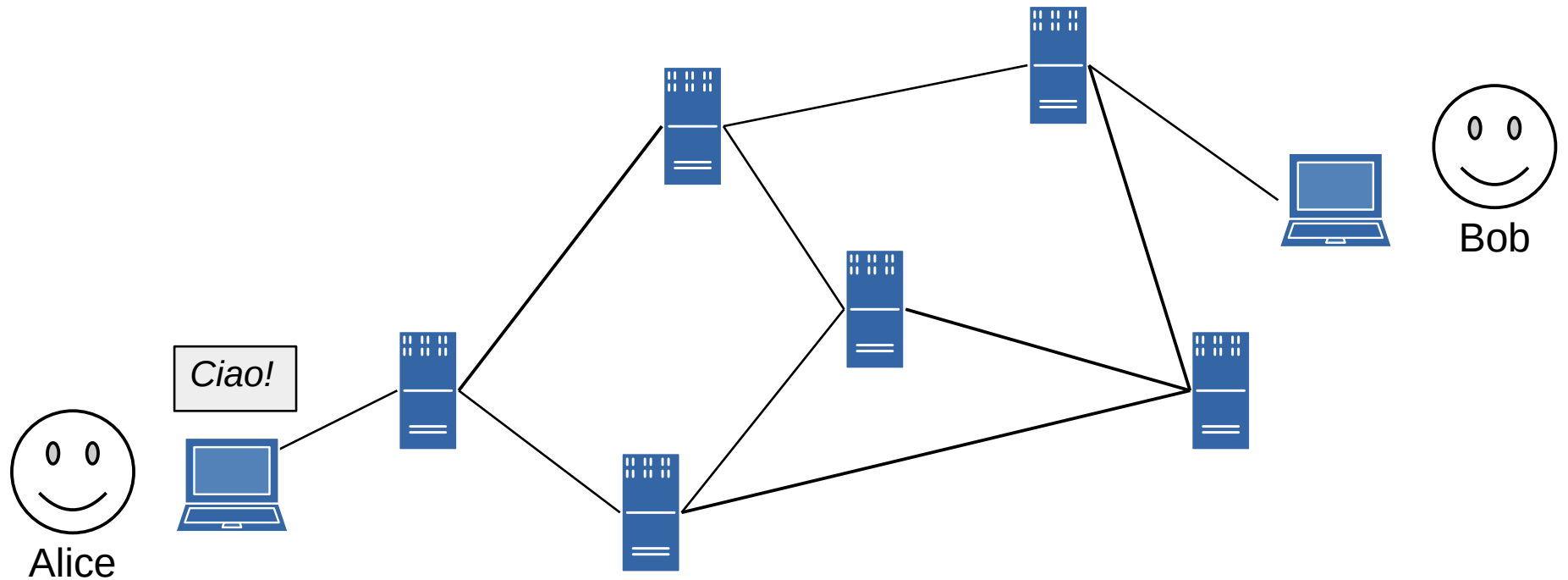
Un utente non è in grado di determinare con certezza il mittente di un messaggio.



Evil Icon by <https://iconsmind.com>

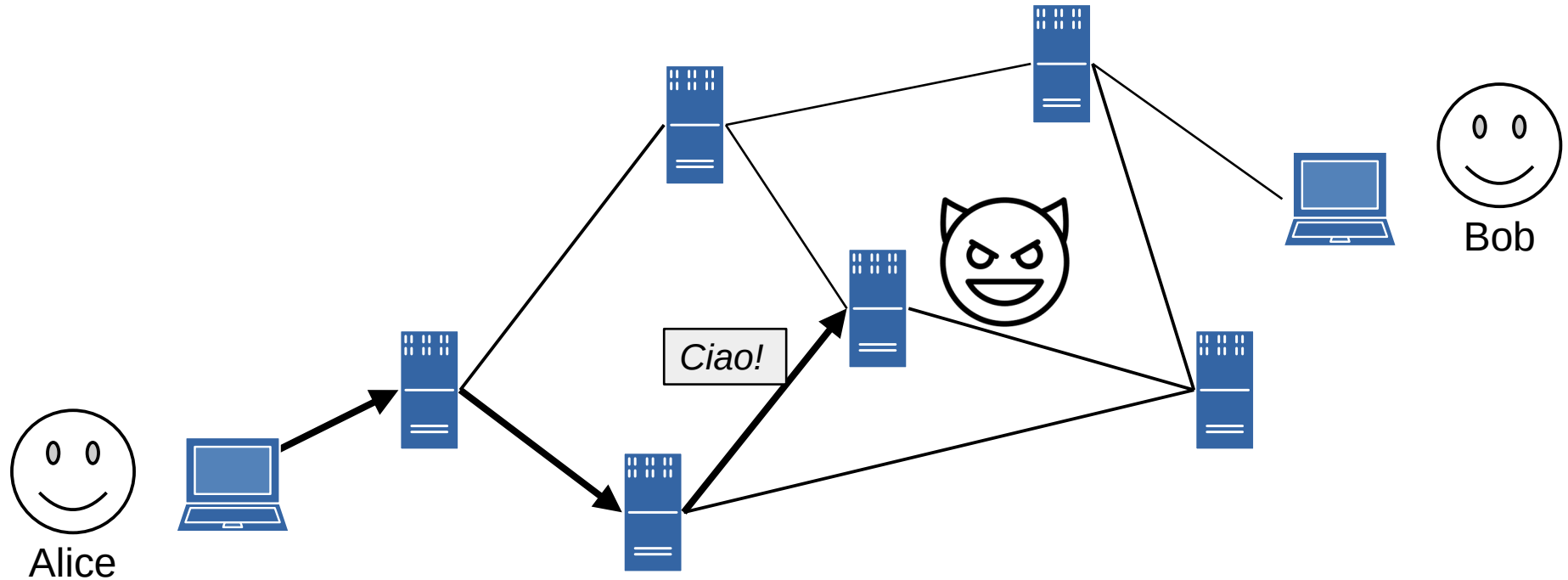
Autenticità e integrità

Quando inviamo un messaggio (pacchetto) ...



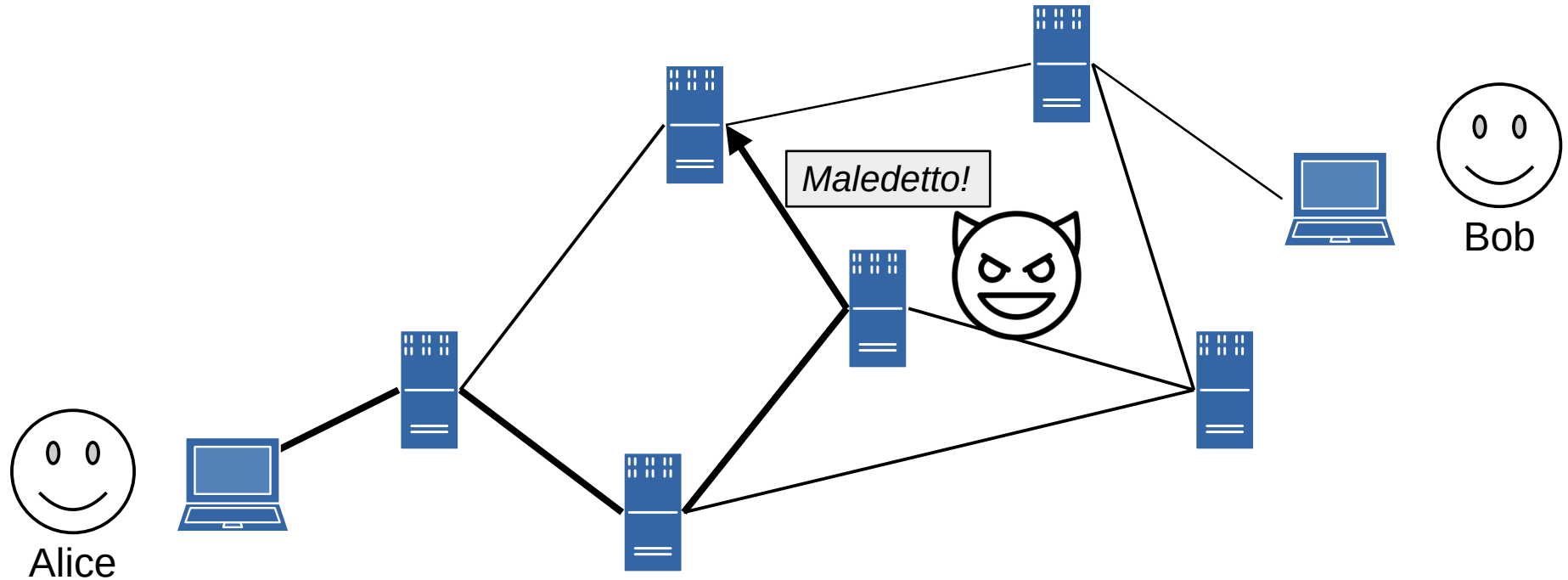
Autenticità e integrità

Quando inviamo un messaggio (pacchetto) molte persone potrebbero alterarlo prima che arrivi a destinazione



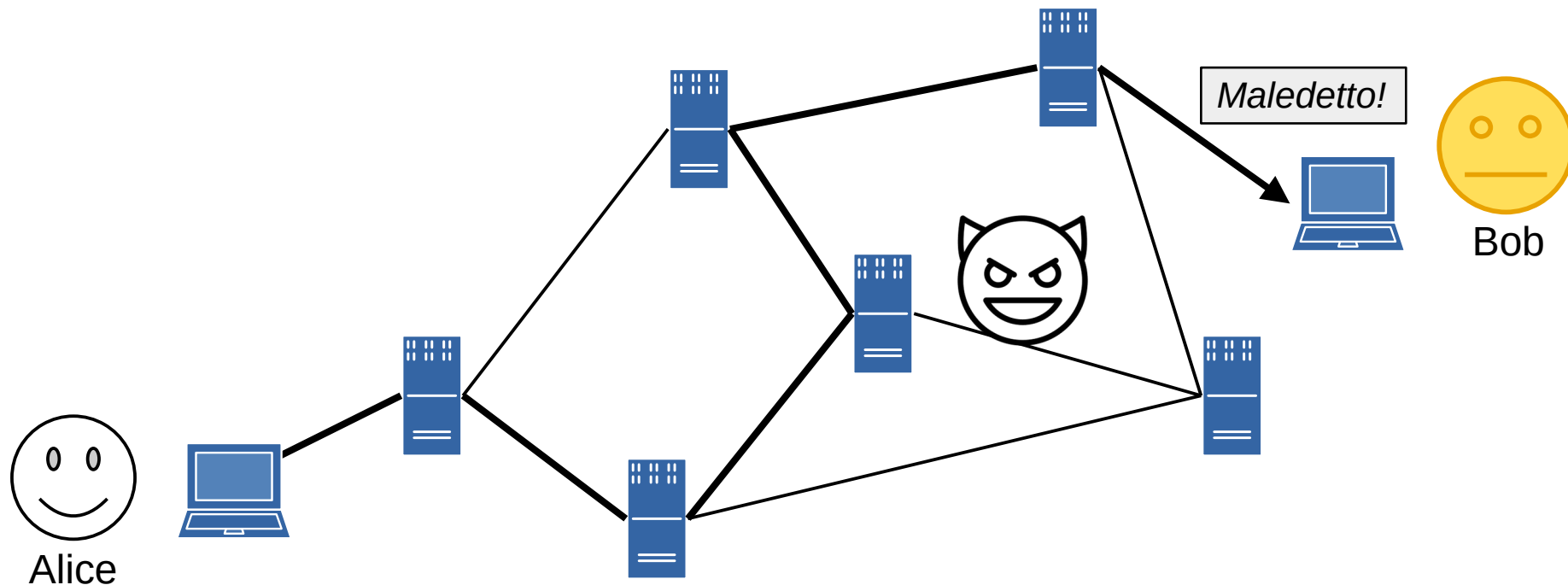
Autenticità e integrità

Quando inviamo un messaggio (pacchetto) molte persone potrebbero alterarlo prima che arrivi a destinazione



Autenticità e integrità

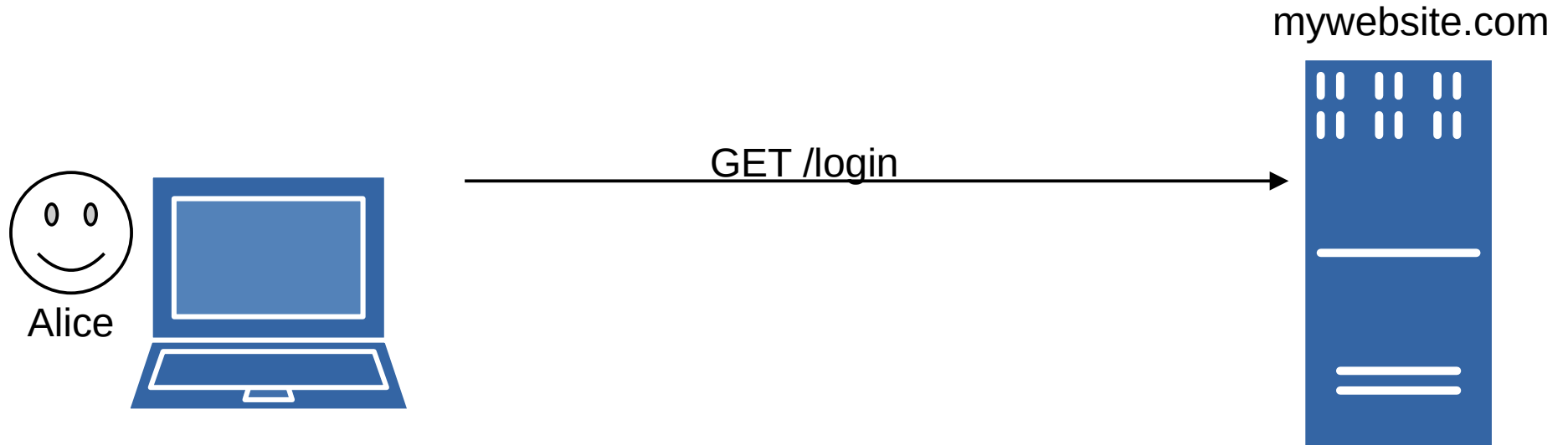
Quando inviamo un messaggio (pacchetto) molte persone potrebbero alterarlo prima che arrivi a destinazione



Phishing - autenticazione

Phishing (da *fishing*, pescare) è un attacco per rubare le credenziali di accesso a un sito. Vediamo un esempio basato su HTTP. Nel processo di autenticazione *classico*

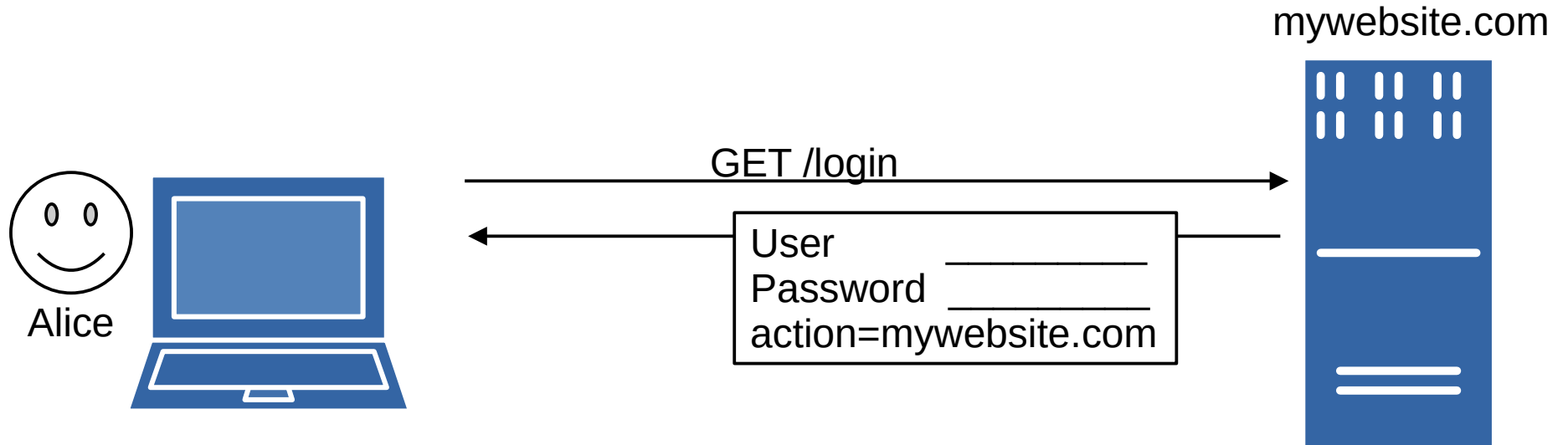
1) L'utente richiede la pagina di *login* al server,



Phishing - autenticazione

Phishing (da *fishing*, pescare) è un attacco per rubare le credenziali di accesso a un sito. Vediamo un esempio basato su HTTP. Nel processo di autenticazione *classico*

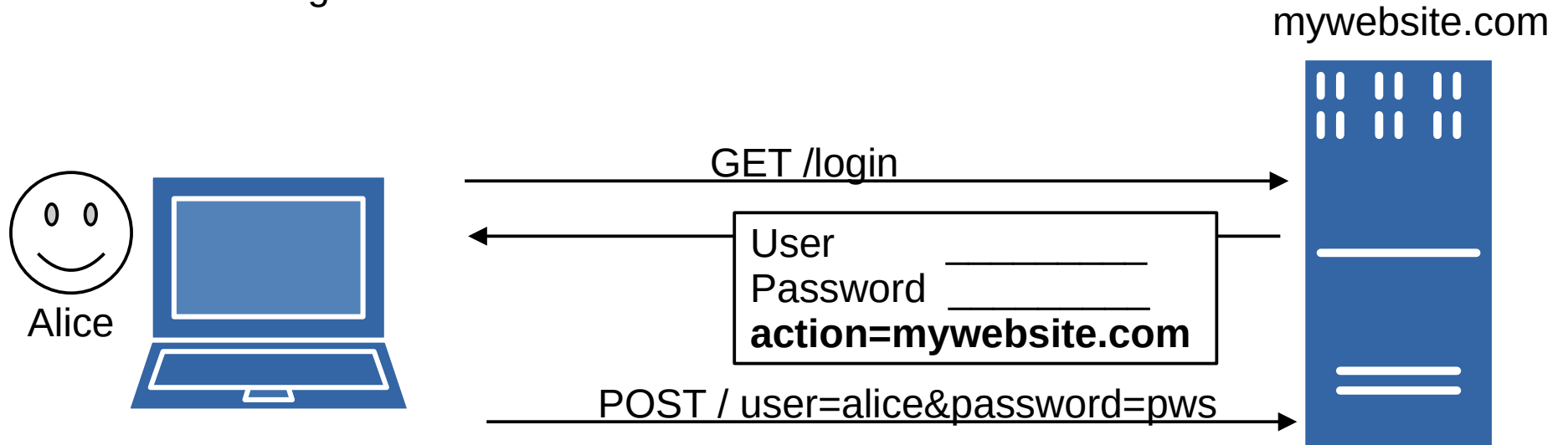
- 1) L'utente richiede la pagina di *login* al server,
- 2) Il server restituisce una *form* di login,



Phishing - autenticazione

Phishing (da *fishing*, pescare) è un attacco per rubare le credenziali di accesso a un sito. Vediamo un esempio basato su HTTP. Nel processo di autenticazione *classico*

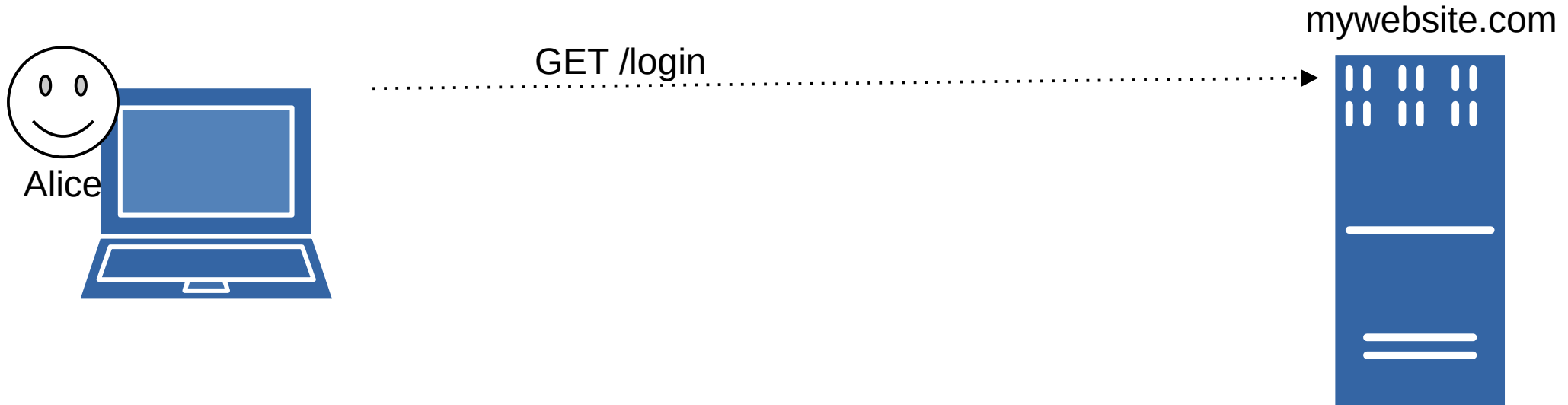
- 1) L'utente richiede la pagina di *login* al server,
- 2) Il server restituisce una *form* di login,
- 3) La form, tra le altre cose, contiene una *action* che indica l'indirizzo a cui inviare i dati di login



Phishing - attacco

In un attacco di tipo phishing

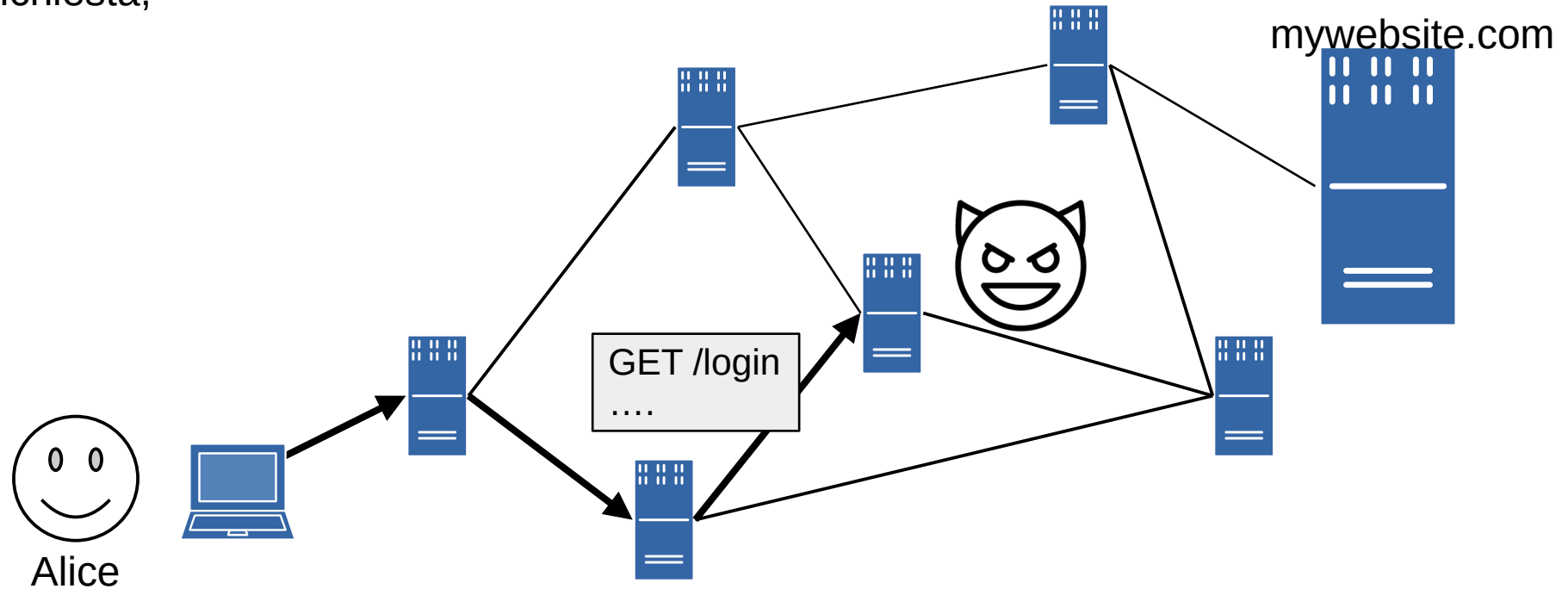
1) L'utente richiede la pagina di *login* al server



Phishing - attacco

In un attacco di tipo phishing

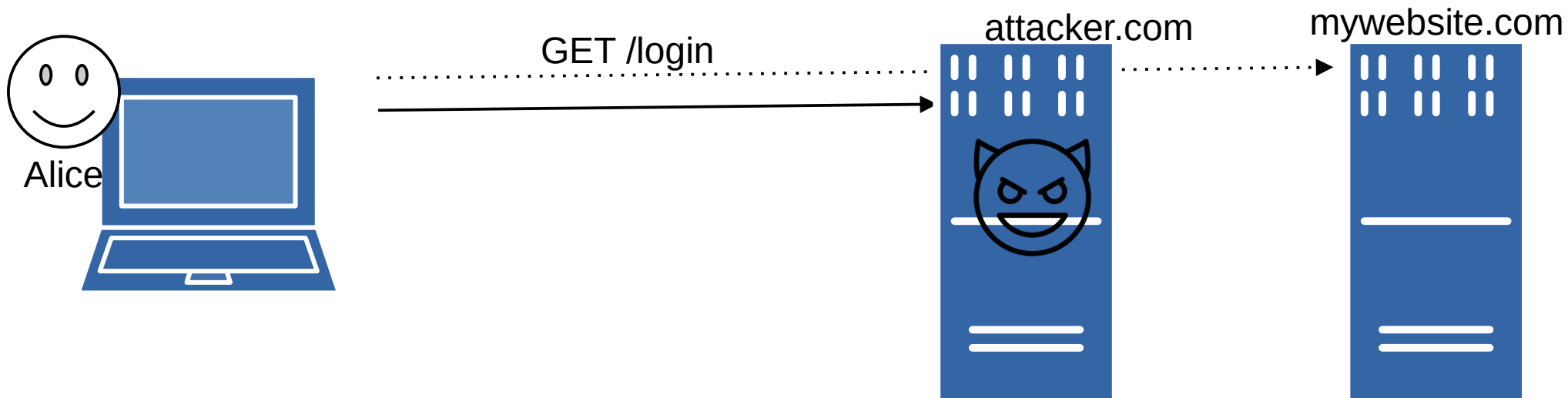
1) L'utente richiede la pagina di *login* al server, ma l'attaccante intercetta la richiesta,



Phishing - attacco

In un attacco di tipo phishing

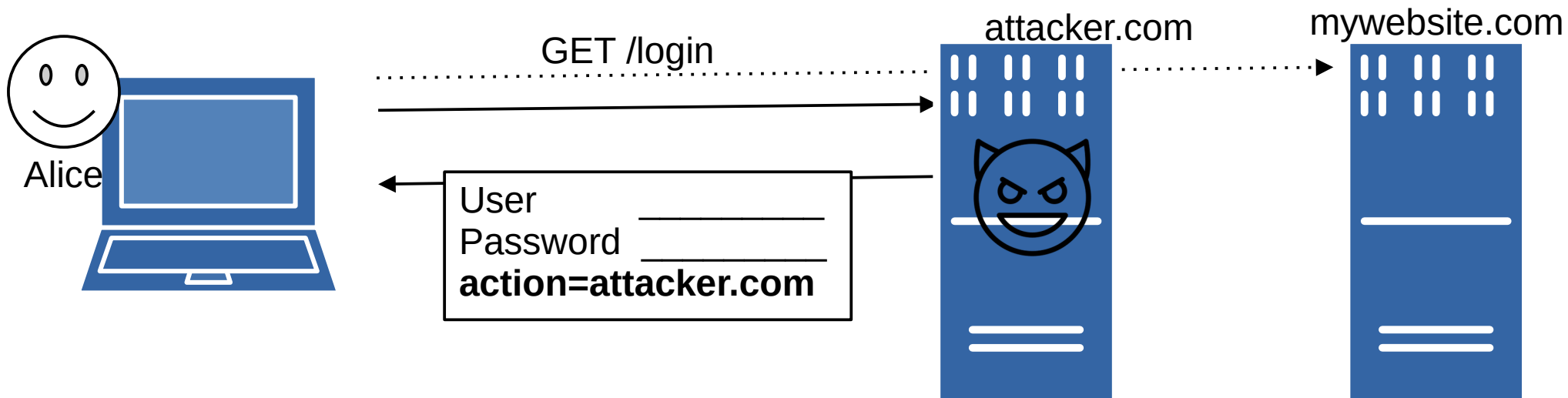
1) L'utente richiede la pagina di *login* al server, ma l'attaccante intercetta la richiesta.



Phishing - attacco

In un attacco di tipo phishing

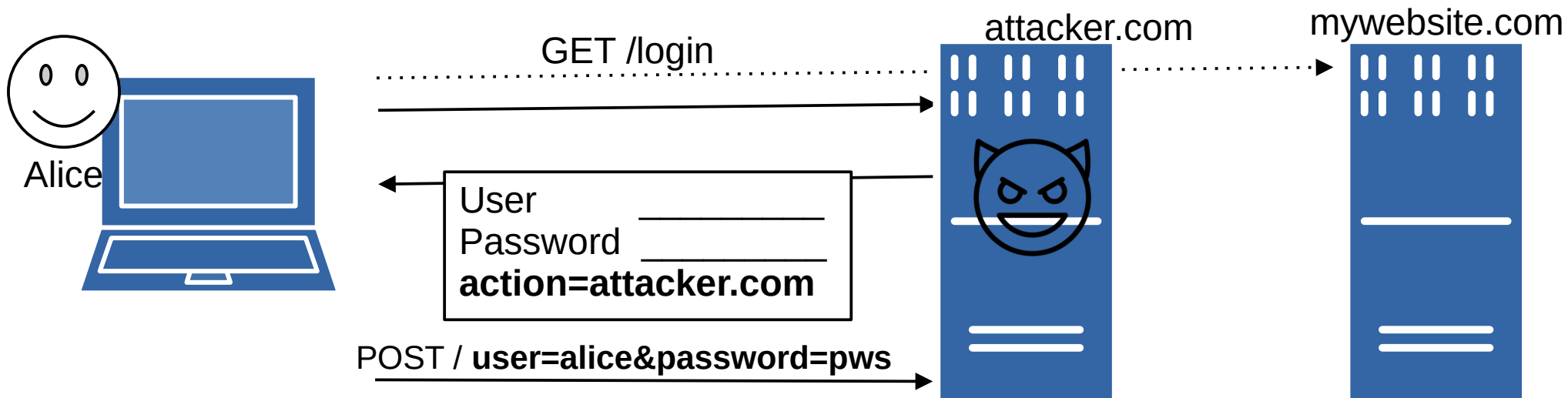
- 1) L'utente richiede la pagina di *login* al server, ma l'attaccante intercetta la richiesta.
- 2) L'attaccante restituisce una *form* di login identica a quella del server, a meno della *action*, che punta ad una propria macchina.



Phishing - attacco

In un attacco di tipo phishing

- 1) L'utente richiede la pagina di *login* al server, ma l'attaccante intercetta la richiesta.
- 2) L'attaccante restituisce una *form* di login identica a quella del server, a meno della *action*, che punta ad una propria macchina.
- 3) L'utente invia le proprie credenziali di login all'indirizzo indicato dall'attaccante.



Crittografia

Alcuni problemi di sicurezza di cui sono affette le reti di computer sono legati

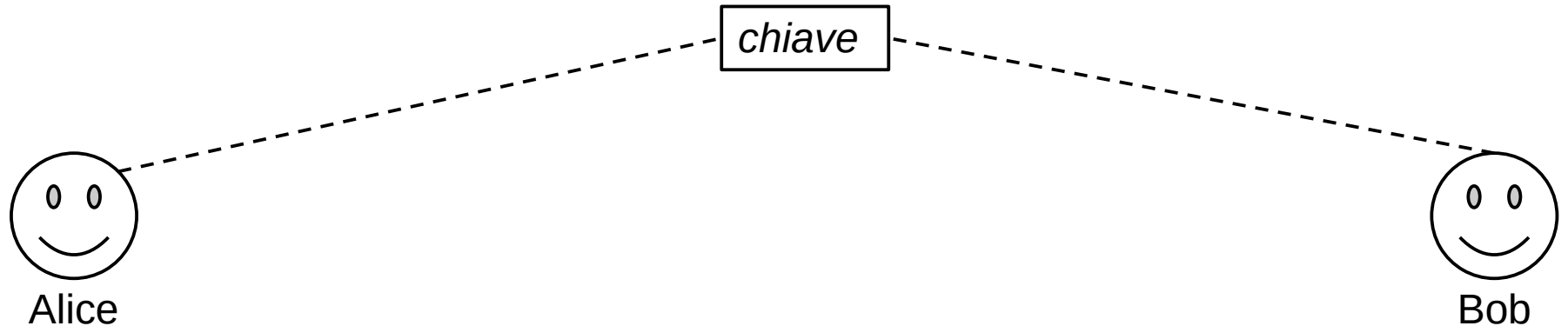
- alla **privacy** (tenere *confidenziali* le proprie attività e i propri dati) e
- all'**autenticità** (essere sicuri del mittente di una comunicazione e che la comunicazione non sia stata alterata).

Questi problemi vengono risolti utilizzando tecniche di **crittografia**, che fornisce metodi per rendere un messaggio non comprensibile a persone non autorizzate a leggerlo.

Vedi anche <https://www.cryptool.org>

Crittografia simmetrica

Le tecniche di **crittografia simmetrica** si basano sulla condivisione di un segreto, detto **chiave**, tra le parti che devono scambiarsi messaggi confidenziali.



Crittografia simmetrica

Le tecniche di **crittografia simmetrica** si basano sulla condivisione di un segreto, detto **chiave**, tra le parti che devono scambiarsi messaggi confidenziali.

L'operazione di **cifratura** genera un *crittotesto* (incomprensibile a chi non conosce la chiave) a partire da un testo originario e la chiave.

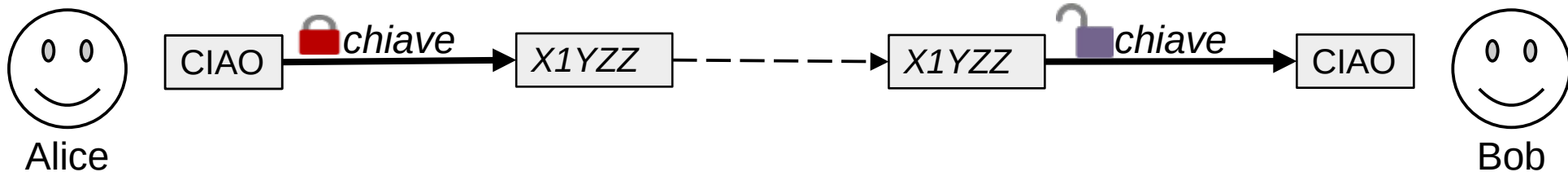


Crittografia simmetrica

Le tecniche di **crittografia simmetrica** si basano sulla condivisione di un segreto, detto **chiave**, tra le parti che devono scambiarsi messaggi confidenziali.

L'operazione di **cifratura** genera un *crittotesto* (incomprensibile a chi non conosce la chiave) a partire da un testo originario (detto *in chiaro*) e la chiave.

La **decifrazione** applica la chiave al crittotesto per restituire il messaggio in chiaro.



Cifrario di Cesare

Il cifrario di Cesare è un sistema di crittografia simmetrica nel quale la chiave è un numero intero.



Vedi anche <https://www.andreaminini.org/crittografia/cifrario-di-cesare-online>

Cifrario di Cesare

Il cifrario di Cesare è un sistema di crittografia simmetrica nel quale la chiave è un numero intero. Supponiamo di avere a disposizione un alfabeto di m caratteri da utilizzare nei messaggi (ad esempio 128 per US-ASCII).

Definizione(Modulo): $x \bmod m$ = il resto della divisione di x per m .

$$0 \bmod 3 = 0$$

$$1 \bmod 3 = 1$$

$$2 \bmod 3 = 2$$

$$3 \bmod 3 = 0$$

$$4 \bmod 3 = 1$$

$$5 \bmod 3 = 2$$

$$6 \bmod 3 = 0$$

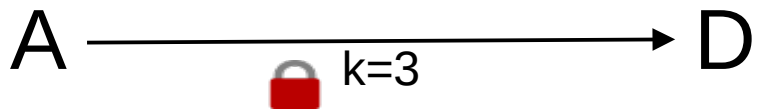
$$7 \bmod 3 = 1$$

Cifrario di Cesare

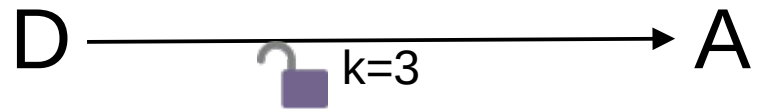
Il cifrario di Cesare è un sistema di crittografia simmetrica nel quale la chiave è un numero intero. Supponiamo di avere a disposizione un alfabeto di m caratteri da utilizzare nei messaggi (ad esempio 128 per US-ASCII).

Definizione(Modulo): $x \bmod m$ = il resto della divisione di x per m .

La cifratura avviene su ogni singolo carattere: $\text{cif}(c,k) = (c + k) \bmod m$.



La decifrazione è l'inverso della cifratura: $\text{dec}(c,k) = (c - k) \bmod m$.



Cifrario di Cesare - esempio

Consideriamo un file di testo con codifica US-ASCII (m=128), contenente "CIAO~".

	30	40	50	60	70	80	90	100	110	120
0:	(2	<	F	P	Z	d	n	x	
1:)	3	=	G	Q	[e	o	y	
2:	*	4	>	H	R	\	f	p	z	
3:	!	+	5	?	I	S]	g	q	{
4:	"	,	6	@	J	T	^	h	r	
5:	#	-	7	A	K	U	_	i	s	}
6:	\$.	8	B	L	V	`	j	t	~
7:	%	/	9	C	M	W	a	k	u	
8:	&	0	:	D	N	X	b	l	v	
9:	'	1	;	E	O	Y	c	m	w	

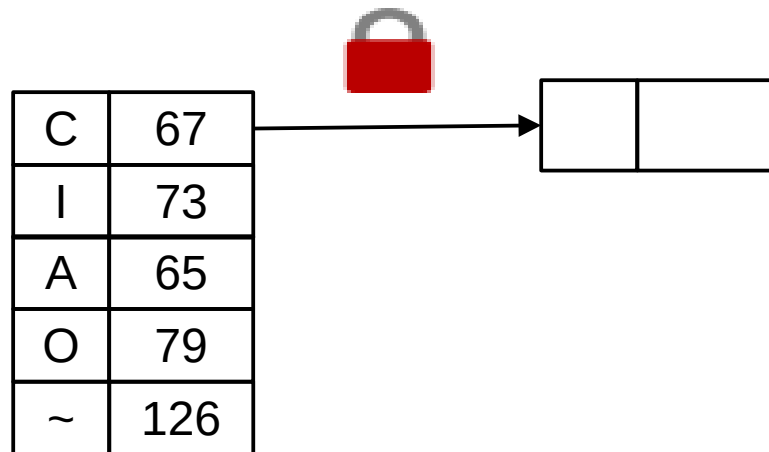
C	67
I	70
A	65
O	79
~	126

Cifrario di Cesare - esempio

Consideriamo un file di testo con codifica US-ASCII (m=128), contenente "CIAO~".
Supponiamo di volerlo codificare con chiave k=37. La codifica avviene un carattere alla volta.

$$\text{cif}(67,37)=(67+37) \bmod 128=$$

	30	40	50	60	70	80	90	100	110	120
0:	(2	<	F	P	Z	d	n	x	
1:)	3	=	G	Q	[e	o	y	
2:	*	4	>	H	R	\	f	p	z	
3:	!	+	5	?	I	S]	g	q	{
4:	"	,	6	@	J	T	^	h	r	
5:	#	-	7	A	K	U	_	i	s	}
6:	\$.	8	B	L	V	`	j	t	~
7:	%	/	9	C	M	W	a	k	u	
8:	&	0	:	D	N	X	b	l	v	
9:	'	1	;	E	O	Y	c	m	w	

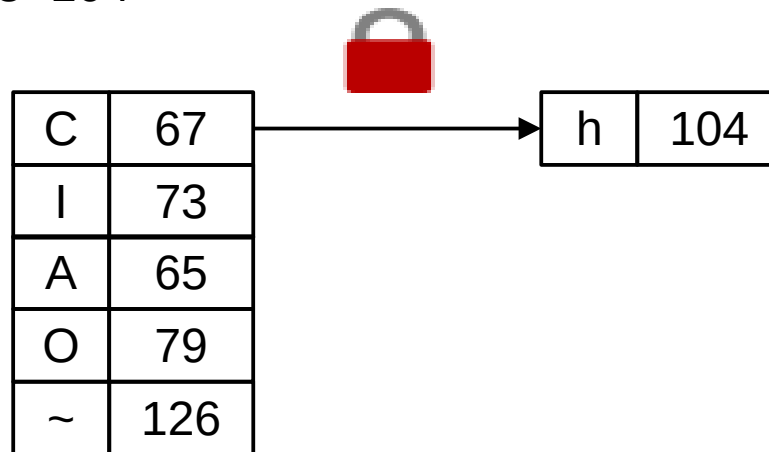


Cifrario di Cesare - esempio

Consideriamo un file di testo con codifica US-ASCII (m=128), contenente "CIAO~".
Supponiamo di volerlo codificare con chiave k=37. La codifica avviene un carattere alla volta.

$$\text{cif}(67,37)=(67+37) \bmod 128=104 \bmod 128=104$$

	30	40	50	60	70	80	90	100	110	120
0:	(2	<	F	P	Z	d	n	x	
1:)	3	=	G	Q	[e	o	y	
2:	*	4	>	H	R	\	f	p	z	
3:	!	+	5	?	I	S]	g	q	{
4:	"	,	6	@	J	T	^	h	r	
5:	#	-	7	A	K	U	_	i	s	}
6:	\$.	8	B	L	V	`	j	t	~
7:	%	/	9	C	M	W	a	k	u	
8:	&	0	:	D	N	X	b	l	v	
9:	'	1	;	E	O	Y	c	m	w	

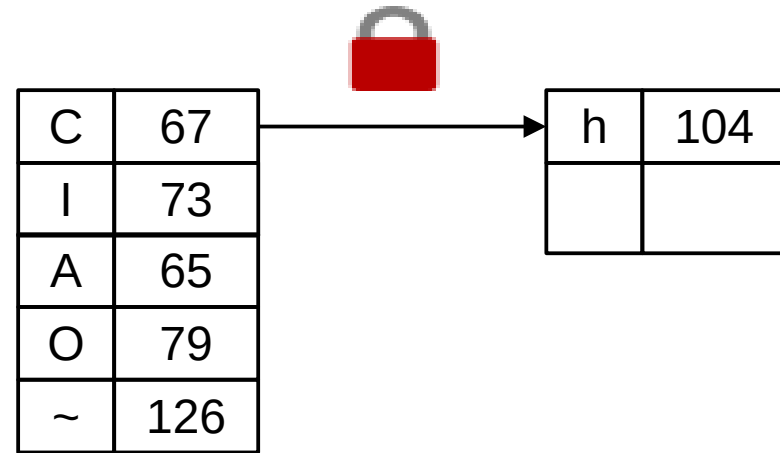


Cifrario di Cesare - esempio

Consideriamo un file di testo con codifica US-ASCII (m=128), contenente "CIAO~".
Supponiamo di volerlo codificare con chiave k=37. La codifica avviene un carattere alla volta.

$\text{cif}(73,37)=$

	30	40	50	60	70	80	90	100	110	120
0:	(2	<	F	P	Z	d	n	x	
1:)	3	=	G	Q	[e	o	y	
2:	*	4	>	H	R	\	f	p	z	
3:	!	+	5	?	I	S]	g	q	{
4:	"	,	6	@	J	T	^	h	r	
5:	#	-	7	A	K	U	_	i	s	}
6:	\$.	8	B	L	V	`	j	t	~
7:	%	/	9	C	M	W	a	k	u	
8:	&	0	:	D	N	X	b	l	v	
9:	'	1	;	E	O	Y	c	m	w	

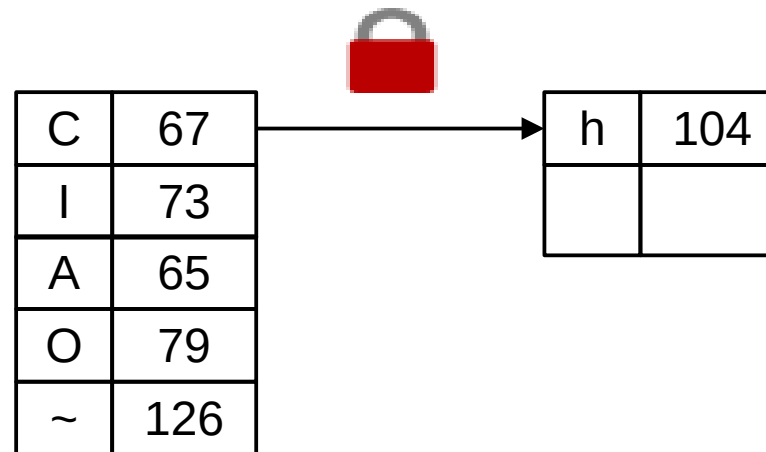


Cifrario di Cesare - esempio

Consideriamo un file di testo con codifica US-ASCII (m=128), contenente "CIAO~".
Supponiamo di volerlo codificare con chiave k=37. La codifica avviene un carattere alla volta.

$$\text{cif}(73,37)=(73+37) \bmod 128$$

	30	40	50	60	70	80	90	100	110	120
0:	(2	<	F	P	Z	d	n	x	
1:)	3	=	G	Q	[e	o	y	
2:	*	4	>	H	R	\	f	p	z	
3:	!	+	5	?	I	S]	g	q	{
4:	"	,	6	@	J	T	^	h	r	
5:	#	-	7	A	K	U	_	i	s	}
6:	\$.	8	B	L	V	`	j	t	~
7:	%	/	9	C	M	W	a	k	u	
8:	&	0	:	D	N	X	b	l	v	
9:	'	1	;	E	O	Y	c	m	w	

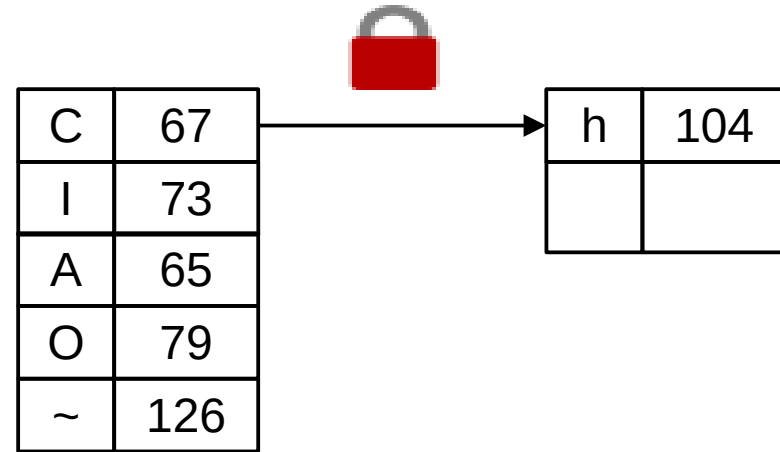


Cifrario di Cesare - esempio

Consideriamo un file di testo con codifica US-ASCII (m=128), contenente "CIAO~".
Supponiamo di volerlo codificare con chiave k=37. La codifica avviene un carattere alla volta.

$$\text{cif}(73,37)=(73+37) \bmod 128=110 \bmod 128$$

	30	40	50	60	70	80	90	100	110	120
0:	(2	<	F	P	Z	d	n	x	
1:)	3	=	G	Q	[e	o	y	
2:	*	4	>	H	R	\	f	p	z	
3:	!	+	5	?	I	S]	g	q	{
4:	"	,	6	@	J	T	^	h	r	
5:	#	-	7	A	K	U	_	i	s	}
6:	\$.	8	B	L	V	`	j	t	~
7:	%	/	9	C	M	W	a	k	u	
8:	&	0	:	D	N	X	b	l	v	
9:	'	1	;	E	O	Y	c	m	w	

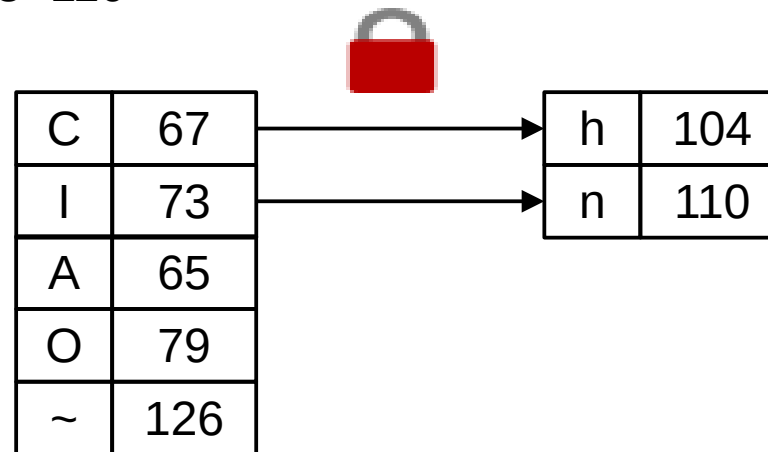


Cifrario di Cesare - esempio

Consideriamo un file di testo con codifica US-ASCII (m=128), contenente "CIAO~".
Supponiamo di volerlo codificare con chiave k=37. La codifica avviene un carattere alla volta.

$$\text{cif}(73,37)=(73+37) \bmod 128=110 \bmod 128=110$$

	30	40	50	60	70	80	90	100	110	120
0:	(2	<	F	P	Z	d	n	x	
1:)	3	=	G	Q	[e	o	y	
2:	*	4	>	H	R	\	f	p	z	
3:	!	+	5	?	I	S]	g	q	{
4:	"	,	6	@	J	T	^	h	r	
5:	#	-	7	A	K	U	_	i	s	}
6:	\$.	8	B	L	V	`	j	t	~
7:	%	/	9	C	M	W	a	k	u	
8:	&	0	:	D	N	X	b	l	v	
9:	'	1	;	E	O	Y	c	m	w	

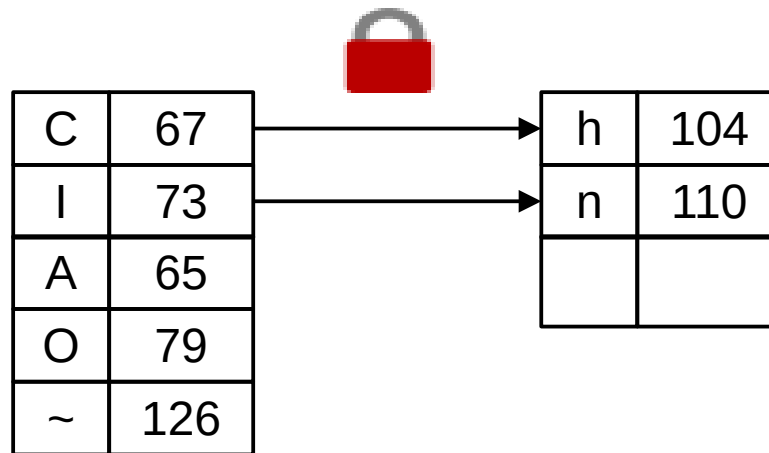


Cifrario di Cesare - esempio

Consideriamo un file di testo con codifica US-ASCII (m=128), contenente "CIAO~".
Supponiamo di volerlo codificare con chiave k=37. La codifica avviene un carattere alla volta.

$$\text{cif}(65,37)=(65+37) \bmod 128$$

	30	40	50	60	70	80	90	100	110	120
0:	(2	<	F	P	Z	d	n	x	
1:)	3	=	G	Q	[e	o	y	
2:	*	4	>	H	R	\	f	p	z	
3:	!	+	5	?	I	S]	g	q	{
4:	"	,	6	@	J	T	^	h	r	
5:	#	-	7	A	K	U	_	i	s	}
6:	\$.	8	B	L	V	`	j	t	~
7:	%	/	9	C	M	W	a	k	u	
8:	&	0	:	D	N	X	b	l	v	
9:	'	1	;	E	O	Y	c	m	w	

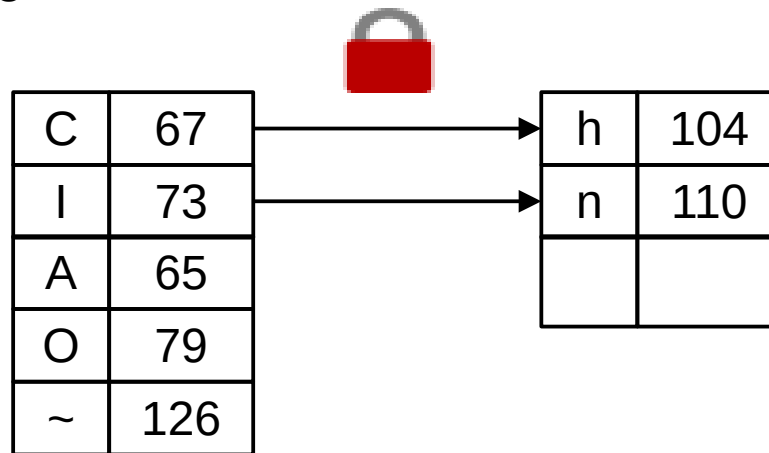


Cifrario di Cesare - esempio

Consideriamo un file di testo con codifica US-ASCII (m=128), contenente "CIAO~".
Supponiamo di volerlo codificare con chiave k=37. La codifica avviene un carattere alla volta.

$$\text{cif}(65,37)=(65+37) \bmod 128=102 \bmod 128$$

	30	40	50	60	70	80	90	100	110	120
0:	(2	<	F	P	Z	d	n	x	
1:)	3	=	G	Q	[e	o	y	
2:	*	4	>	H	R	\	f	p	z	
3:	!	+	5	?	I	S]	g	q	{
4:	"	,	6	@	J	T	^	h	r	
5:	#	-	7	A	K	U	_	i	s	}
6:	\$.	8	B	L	V	`	j	t	~
7:	%	/	9	C	M	W	a	k	u	
8:	&	0	:	D	N	X	b	l	v	
9:	'	1	;	E	O	Y	c	m	w	

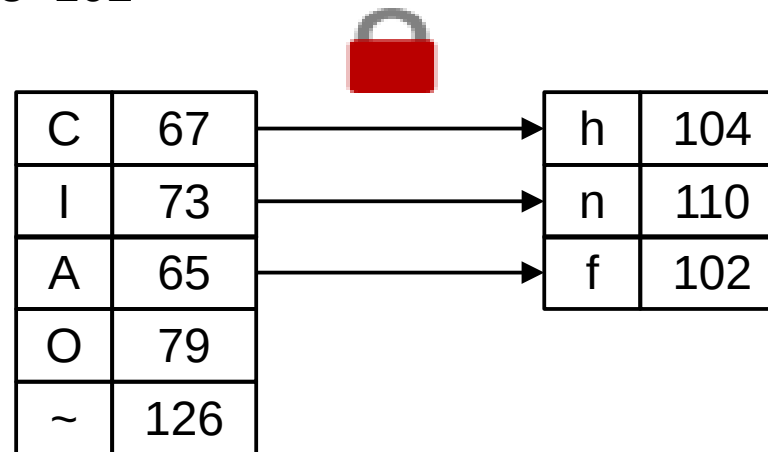


Cifrario di Cesare - esempio

Consideriamo un file di testo con codifica US-ASCII (m=128), contenente "CIAO~".
Supponiamo di volerlo codificare con chiave k=37. La codifica avviene un carattere alla volta.

$$\text{cif}(65,37)=(65+37) \bmod 128=102 \bmod 128=102$$

	30	40	50	60	70	80	90	100	110	120
0:	(2	<	F	P	Z	d	n	x	
1:)	3	=	G	Q	[e	o	y	
2:	*	4	>	H	R	\	f	p	z	
3:	!	+	5	?	I	S]	g	q	{
4:	"	,	6	@	J	T	^	h	r	
5:	#	-	7	A	K	U	_	i	s	}
6:	\$.	8	B	L	V	`	j	t	~
7:	%	/	9	C	M	W	a	k	u	
8:	&	0	:	D	N	X	b	l	v	
9:	'	1	;	E	O	Y	c	m	w	

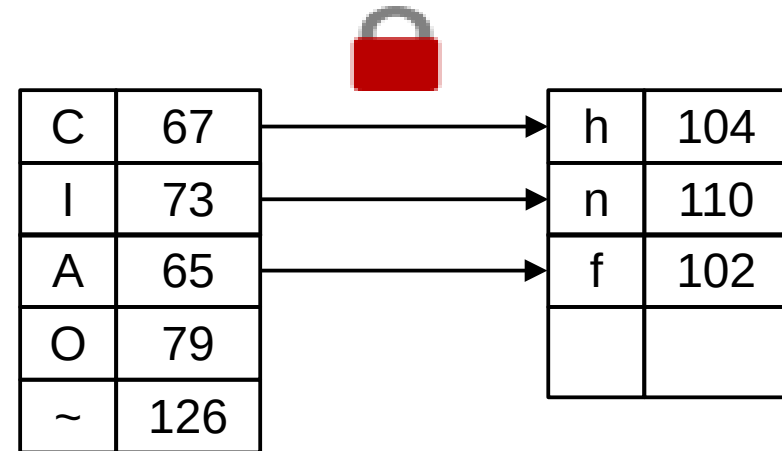


Cifrario di Cesare - esempio

Consideriamo un file di testo con codifica US-ASCII (m=128), contenente "CIAO~".
Supponiamo di volerlo codificare con chiave k=37. La codifica avviene un carattere alla volta.

$\text{cif}(79,37)=$

	30	40	50	60	70	80	90	100	110	120
0:	(2	<	F	P	Z	d	n	x	
1:)	3	=	G	Q	[e	o	y	
2:	*	4	>	H	R	\	f	p	z	
3:	!	+	5	?	I	S]	g	q	{
4:	"	,	6	@	J	T	^	h	r	
5:	#	-	7	A	K	U	_	i	s	}
6:	\$.	8	B	L	V	`	j	t	~
7:	%	/	9	C	M	W	a	k	u	
8:	&	0	:	D	N	X	b	l	v	
9:	'	1	;	E	O	Y	c	m	w	

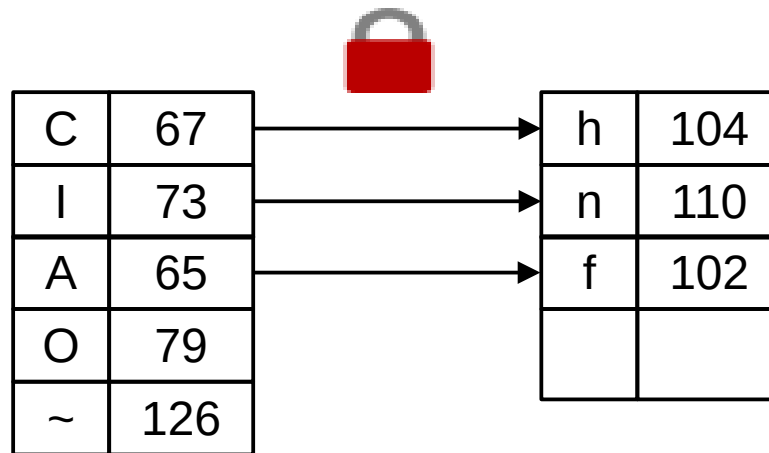


Cifrario di Cesare - esempio

Consideriamo un file di testo con codifica US-ASCII (m=128), contenente "CIAO~".
Supponiamo di volerlo codificare con chiave k=37. La codifica avviene un carattere alla volta.

$$\text{cif}(79,37)=(79+37) \bmod 128$$

	30	40	50	60	70	80	90	100	110	120
0:	(2	<	F	P	Z	d	n	x	
1:)	3	=	G	Q	[e	o	y	
2:	*	4	>	H	R	\	f	p	z	
3:	!	+	5	?	I	S]	g	q	{
4:	"	,	6	@	J	T	^	h	r	
5:	#	-	7	A	K	U	_	i	s	}
6:	\$.	8	B	L	V	`	j	t	~
7:	%	/	9	C	M	W	a	k	u	
8:	&	0	:	D	N	X	b	l	v	
9:	'	1	;	E	O	Y	c	m	w	

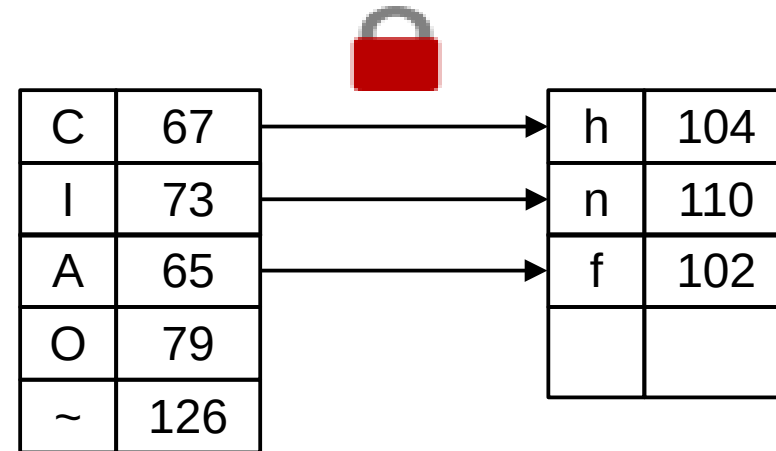


Cifrario di Cesare - esempio

Consideriamo un file di testo con codifica US-ASCII (m=128), contenente "CIAO~".
Supponiamo di volerlo codificare con chiave k=37. La codifica avviene un carattere alla volta.

$$\text{cif}(79,37)=(79+37) \bmod 128=116 \bmod 128$$

	30	40	50	60	70	80	90	100	110	120
0:	(2	<	F	P	Z	d	n	x	
1:)	3	=	G	Q	[e	o	y	
2:	*	4	>	H	R	\	f	p	z	
3:	!	+	5	?	I	S]	g	q	{
4:	"	,	6	@	J	T	^	h	r	
5:	#	-	7	A	K	U	_	i	s	}
6:	\$.	8	B	L	V	`	j	t	~
7:	%	/	9	C	M	W	a	k	u	
8:	&	0	:	D	N	X	b	l	v	
9:	'	1	;	E	O	Y	c	m	w	

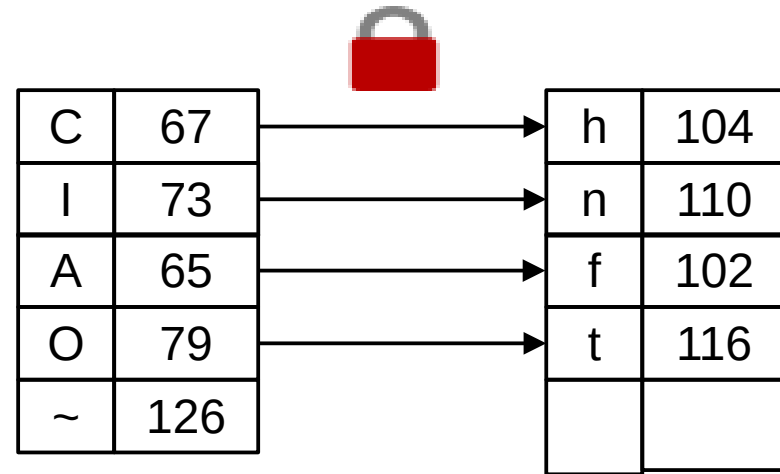


Cifrario di Cesare - esempio

Consideriamo un file di testo con codifica US-ASCII (m=128), contenente "CIAO~".
Supponiamo di volerlo codificare con chiave k=37. La codifica avviene un carattere alla volta.

$$\text{cif}(79,37)=(79+37) \bmod 128=116 \bmod 128=116$$

	30	40	50	60	70	80	90	100	110	120
0:	(2	<	F	P	Z	d	n	x	
1:)	3	=	G	Q	[e	o	y	
2:	*	4	>	H	R	\	f	p	z	
3:	!	+	5	?	I	S]	g	q	{
4:	"	,	6	@	J	T	^	h	r	
5:	#	-	7	A	K	U	_	i	s	}
6:	\$.	8	B	L	V	`	j	t	~
7:	%	/	9	C	M	W	a	k	u	
8:	&	0	:	D	N	X	b	l	v	
9:	'	1	;	E	O	Y	c	m	w	

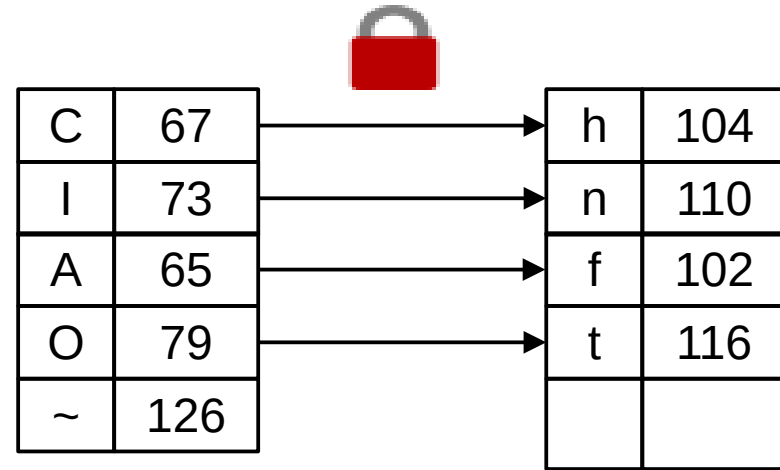


Cifrario di Cesare - esempio

Consideriamo un file di testo con codifica US-ASCII (m=128), contenente "CIAO~".
Supponiamo di volerlo codificare con chiave k=37. La codifica avviene un carattere alla volta.

$\text{cif}(126,37)=$

	30	40	50	60	70	80	90	100	110	120
0:	(2	<	F	P	Z	d	n	x	
1:)	3	=	G	Q	[e	o	y	
2:	*	4	>	H	R	\	f	p	z	
3:	!	+	5	?	I	S]	g	q	{
4:	"	,	6	@	J	T	^	h	r	
5:	#	-	7	A	K	U	_	i	s	}
6:	\$.	8	B	L	V	`	j	t	~
7:	%	/	9	C	M	W	a	k	u	
8:	&	0	:	D	N	X	b	l	v	
9:	'	1	;	E	O	Y	c	m	w	

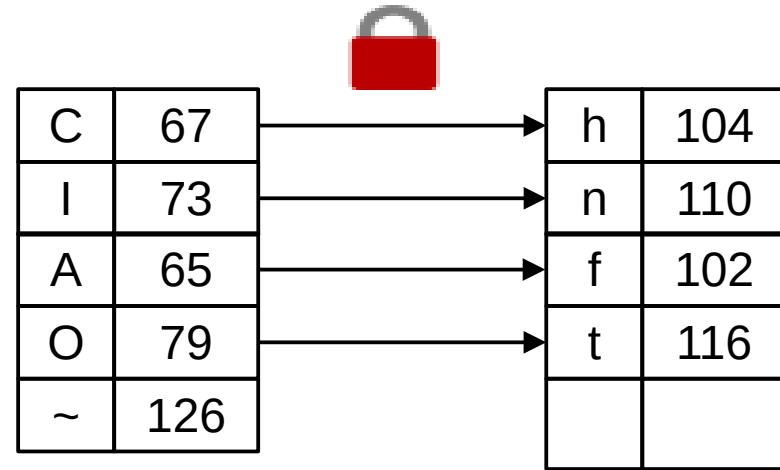


Cifrario di Cesare - esempio

Consideriamo un file di testo con codifica US-ASCII (m=128), contenente "CIAO~".
Supponiamo di volerlo codificare con chiave k=37. La codifica avviene un carattere alla volta.

$$\text{cif}(126,37)=(126+37) \bmod 128$$

	30	40	50	60	70	80	90	100	110	120
0:	(2	<	F	P	Z	d	n	x	
1:)	3	=	G	Q	[e	o	y	
2:	*	4	>	H	R	\	f	p	z	
3:	!	+	5	?	I	S]	g	q	{
4:	"	,	6	@	J	T	^	h	r	
5:	#	-	7	A	K	U	_	i	s	}
6:	\$.	8	B	L	V	`	j	t	~
7:	%	/	9	C	M	W	a	k	u	
8:	&	0	:	D	N	X	b	l	v	
9:	'	1	;	E	O	Y	c	m	w	

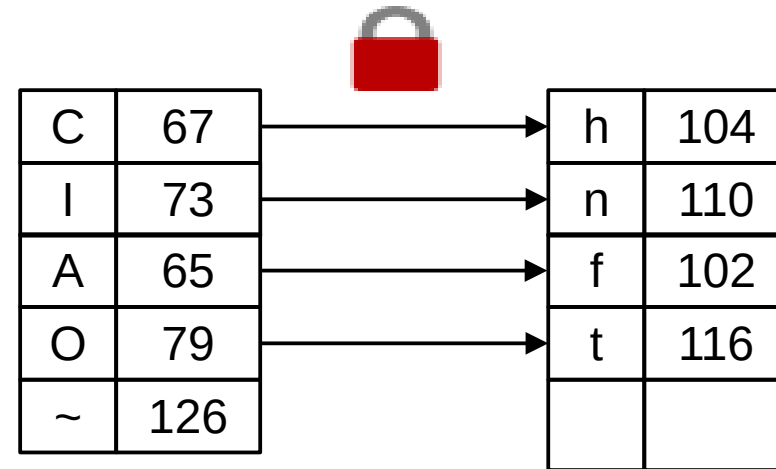


Cifrario di Cesare - esempio

Consideriamo un file di testo con codifica US-ASCII (m=128), contenente "CIAO~".
Supponiamo di volerlo codificare con chiave k=37. La codifica avviene un carattere alla volta.

$$\text{cif}(126,37)=(126+37) \bmod 128=163 \bmod 128$$

	30	40	50	60	70	80	90	100	110	120
0:	(2	<	F	P	Z	d	n	x	
1:)	3	=	G	Q	[e	o	y	
2:	*	4	>	H	R	\	f	p	z	
3:	!	+	5	?	I	S]	g	q	{
4:	"	,	6	@	J	T	^	h	r	
5:	#	-	7	A	K	U	_	i	s	}
6:	\$.	8	B	L	V	`	j	t	~
7:	%	/	9	C	M	W	a	k	u	
8:	&	0	:	D	N	X	b	l	v	
9:	'	1	;	E	O	Y	c	m	w	

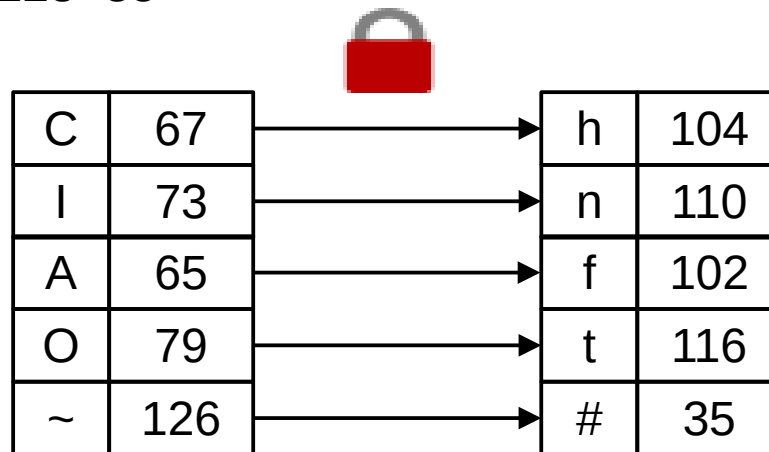


Cifrario di Cesare - esempio

Consideriamo un file di testo con codifica US-ASCII (m=128), contenente "CIAO~".
Supponiamo di volerlo codificare con chiave k=37. La codifica avviene un carattere alla volta.

$$\text{cif}(126,37)=(126+37) \bmod 128=163 \bmod 128=35$$

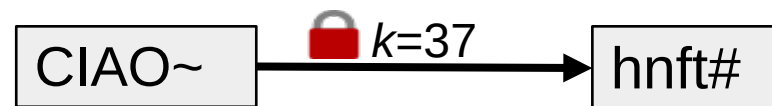
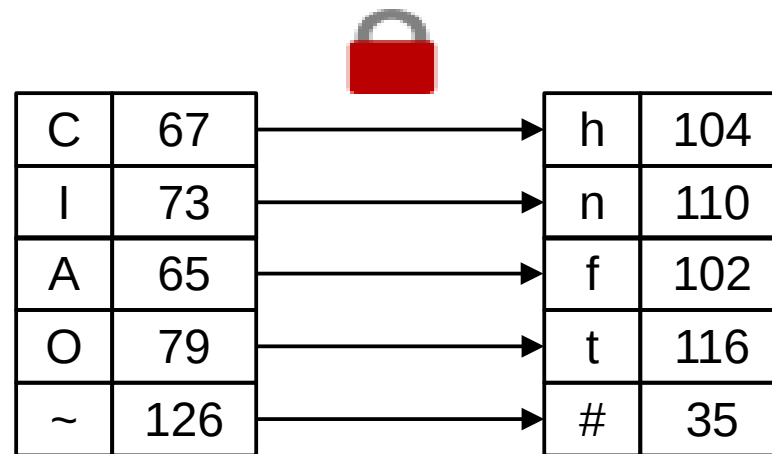
	30	40	50	60	70	80	90	100	110	120
0:	(2	<	F	P	Z	d	n	x	
1:)	3	=	G	Q	[e	o	y	
2:	*	4	>	H	R	\	f	p	z	
3:	!	+	5	?	I	S]	g	q	{
4:	"	,	6	@	J	T	^	h	r	
5:	#	-	7	A	K	U	_	i	s	}
6:	\$.	8	B	L	V	`	j	t	~
7:	%	/	9	C	M	W	a	k	u	
8:	&	0	:	D	N	X	b	l	v	
9:	'	1	;	E	O	Y	c	m	w	



Cifrario di Cesare - esempio

Consideriamo un file di testo con codifica US-ASCII (m=128), contenente "CIAO~".
Supponiamo di volerlo codificare con chiave k=37. La codifica avviene un carattere alla volta.
I caratteri così ottenuti vengono concatenati.

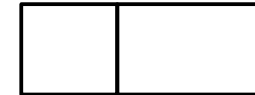
	30	40	50	60	70	80	90	100	110	120
0:	(2	<	F	P	Z	d	n	x	
1:)	3	=	G	Q	[e	o	y	
2:	*	4	>	H	R	\	f	p	z	
3:	!	+	5	?	I	S]	g	q	{
4:	"	,	6	@	J	T	^	h	r	
5:	#	-	7	A	K	U	_	i	s	}
6:	\$.	8	B	L	V	`	j	t	~
7:	%	/	9	C	M	W	a	k	u	
8:	&	0	:	D	N	X	b	l	v	
9:	'	1	;	E	O	Y	c	m	w	



Cifrario di Cesare – esempio - decifrazione

Consideriamo un crittotesto “hnft#” con codifica US-ASCII (m=128). Sapendo che è stato codificato con chiave $k=37$, possiamo ottenere il testo in chiaro. Si procede un carattere alla volta.

$$\text{dec}(104,37)=$$



	30	40	50	60	70	80	90	100	110	120
0:	(2	<	F	P	Z	d	n	x	
1:)	3	=	G	Q	[e	o	y	
2:	*	4	>	H	R	\	f	p	z	
3:	!	+	5	?	I	S]	g	q	{
4:	"	,	6	@	J	T	^	h	r	
5:	#	-	7	A	K	U	_	i	s	}
6:	\$.	8	B	L	V	`	j	t	~
7:	%	/	9	C	M	W	a	k	u	
8:	&	0	:	D	N	X	b	l	v	
9:	'	1	;	E	O	Y	c	m	w	

h	104
n	110
f	102
t	116
#	35

Cifrario di Cesare – esempio - decifrazione

Consideriamo un crittotesto “hkft#” con codifica US-ASCII (m=128). Sapendo che è stato codificato con chiave $k=37$, possiamo ottenere il testo in chiaro. Si procede un carattere alla volta.

$$\text{dec}(104,37)=(104-37) \bmod 128$$



	30	40	50	60	70	80	90	100	110	120
0:	(2	<	F	P	Z	d	n	x	
1:)	3	=	G	Q	[e	o	y	
2:	*	4	>	H	R	\	f	p	z	
3:	!	+	5	?	I	S]	g	q	{
4:	"	,	6	@	J	T	^	h	r	
5:	#	-	7	A	K	U	_	i	s	}
6:	\$.	8	B	L	V	`	j	t	~
7:	%	/	9	C	M	W	a	k	u	
8:	&	0	:	D	N	X	b	l	v	
9:	'	1	;	E	O	Y	c	m	w	

h	104
n	110
f	102
t	116
#	35

Cifrario di Cesare – esempio - decifrazione

Consideriamo un crittogramma “hkft#” con codifica US-ASCII (m=128). Sapendo che è stato codificato con chiave $k=37$, possiamo ottenere il testo in chiaro. Si procede un carattere alla volta.

$$\text{dec}(104,37)=(104-37) \bmod 128=67 \bmod 128$$



	30	40	50	60	70	80	90	100	110	120
0:	(2	<	F	P	Z	d	n	x	
1:)	3	=	G	Q	[e	o	y	
2:	*	4	>	H	R	\	f	p	z	
3:	!	+	5	?	I	S]	g	q	{
4:	"	,	6	@	J	T	^	h	r	
5:	#	-	7	A	K	U	_	i	s	}
6:	\$.	8	B	L	V	`	j	t	~
7:	%	/	9	C	M	W	a	k	u	
8:	&	0	:	D	N	X	b	l	v	
9:	'	1	;	E	O	Y	c	m	w	

h	104
n	110
f	102
t	116
#	35

Cifrario di Cesare – esempio - decifrazione

Consideriamo un crittogramma “hkft#” con codifica US-ASCII (m=128). Sapendo che è stato codificato con chiave $k=37$, possiamo ottenere il testo in chiaro. Si procede un carattere alla volta.

$$\text{dec}(104,37)=(104-37) \bmod 128=67 \bmod 128=67$$



	30	40	50	60	70	80	90	100	110	120
0:	(2	<	F	P	Z	d	n	x	
1:)	3	=	G	Q	[e	o	y	
2:	*	4	>	H	R	\	f	p	z	
3:	!	+	5	?	I	S]	g	q	{
4:	"	,	6	@	J	T	^	h	r	
5:	#	-	7	A	K	U	_	i	s	}
6:	\$.	8	B	L	V	`	j	t	~
7:	%	/	9	C	M	W	a	k	u	
8:	&	0	:	D	N	X	b	l	v	
9:	'	1	;	E	O	Y	c	m	w	

h	104	→	C	67
n	110			
f	102			
t	116			
#	35			

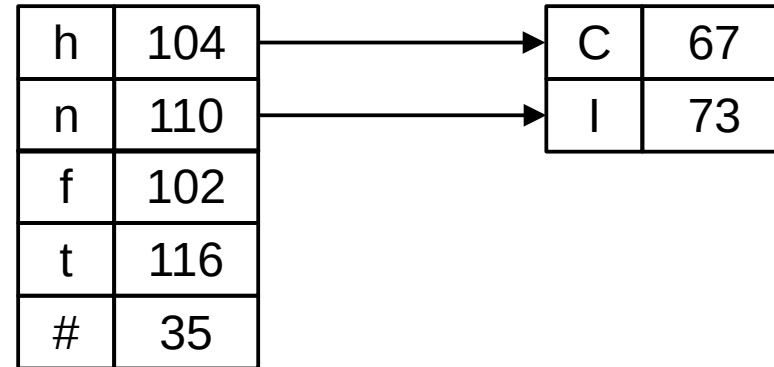
Cifrario di Cesare – esempio - decifrazione

Consideriamo un crittogramma “hkft#” con codifica US-ASCII (m=128). Sapendo che è stato codificato con chiave $k=37$, possiamo ottenere il testo in chiaro. Si procede un carattere alla volta.

$$\text{dec}(110,37)=(110-37) \bmod 128=73 \bmod 128=73$$



	30	40	50	60	70	80	90	100	110	120
0:	(2	<	F	P	Z	d	n	x	
1:)	3	=	G	Q	[e	o	y	
2:	*	4	>	H	R	\	f	p	z	
3:	!	+	5	?	I	S]	g	q	{
4:	"	,	6	@	J	T	^	h	r	
5:	#	-	7	A	K	U	_	i	s	}
6:	\$.	8	B	L	V	`	j	t	~
7:	%	/	9	C	M	W	a	k	u	
8:	&	0	:	D	N	X	b	l	v	
9:	'	1	;	E	O	Y	c	m	w	



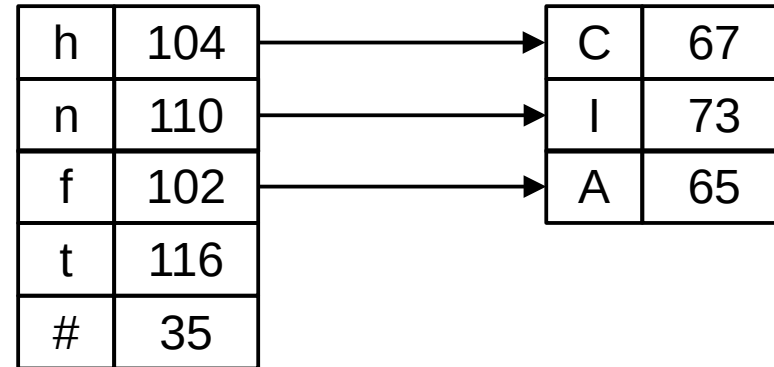
Cifrario di Cesare – esempio - decifrazione

Consideriamo un crittogramma “hkft#” con codifica US-ASCII (m=128). Sapendo che è stato codificato con chiave $k=37$, possiamo ottenere il testo in chiaro. Si procede un carattere alla volta.

$$\text{dec}(102,37)=(102-37) \bmod 128=65 \bmod 128=65$$



	30	40	50	60	70	80	90	100	110	120
0:	(2	<	F	P	Z	d	n	x	
1:)	3	=	G	Q	[e	o	y	
2:	*	4	>	H	R	\	f	p	z	
3:	!	+	5	?	I	S]	g	q	{
4:	"	,	6	@	J	T	^	h	r	
5:	#	-	7	A	K	U	_	i	s	}
6:	\$.	8	B	L	V	`	j	t	~
7:	%	/	9	C	M	W	a	k	u	
8:	&	0	:	D	N	X	b	l	v	
9:	'	1	;	E	O	Y	c	m	w	



Cifrario di Cesare – esempio - decifrazione

Consideriamo un crittotesto “hkft#” con codifica US-ASCII (m=128). Sapendo che è stato codificato con chiave $k=37$, possiamo ottenere il testo in chiaro. Si procede un carattere alla volta.

$$\text{dec}(116,37)=(116-37) \bmod 128=79 \bmod 128=79$$



	30	40	50	60	70	80	90	100	110	120
0:	(2	<	F	P	Z	d	n	x	
1:)	3	=	G	Q	[e	o	y	
2:	*	4	>	H	R	\	f	p	z	
3:	!	+	5	?	I	S]	g	q	{
4:	"	,	6	@	J	T	^	h	r	
5:	#	-	7	A	K	U	_	i	s	}
6:	\$.	8	B	L	V	`	j	t	~
7:	%	/	9	C	M	W	a	k	u	
8:	&	0	:	D	N	X	b	l	v	
9:	'	1	;	E	O	Y	c	m	w	

h	104	→	C	67
n	110	→	I	73
f	102	→	A	65
t	116	→	O	79
#	35			

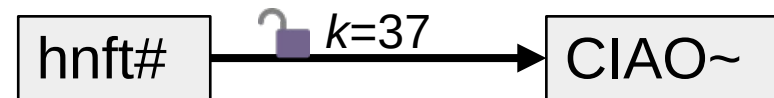
Cifrario di Cesare – esempio - decifrazione

Consideriamo un crittogramma “hnft#” con codifica US-ASCII (m=128). Sapendo che è stato codificato con chiave $k=37$, possiamo ottenere il testo in chiaro. Si procede un carattere alla volta. I caratteri così ottenuti vengono concatenati.



	30	40	50	60	70	80	90	100	110	120
0:	(2	<	F	P	Z	d	n	x	
1:)	3	=	G	Q	[e	o	y	
2:	*	4	>	H	R	\	f	p	z	
3:	!	+	5	?	I	S]	g	q	{
4:	"	,	6	@	J	T	^	h	r	
5:	#	-	7	A	K	U	_	i	s	}
6:	\$.	8	B	L	V	`	j	t	~
7:	%	/	9	C	M	W	a	k	u	
8:	&	0	:	D	N	X	b	l	v	
9:	'	1	;	E	O	Y	c	m	w	

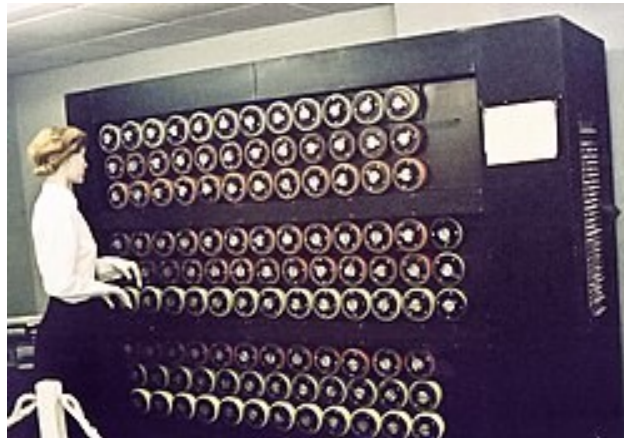
h	104	→	C	67
n	110	→	I	73
f	102	→	A	65
t	116	→	O	79
#	35	→	~	126



Crittoanalisi

La **crittoanalisi** è la disciplina che si occupa di identificare tecniche che permettano la decodifica di messaggi cifrati senza possedere la chiave.

Obiettivo: dato un crittotesto C trovare il testo in chiaro T corrispondente tale che $\text{cif}(T,k)=C$ per qualche k .



Spazio delle chiavi

Spazio delle chiavi: insieme di tutte le possibili chiavi in un sistema di crittografia.

Nel cifrario di Cesare, utilizzato su testi US-ASCII, posso considerare come spazio delle chiavi I numeri interi da 0 a 127, per un totale di 128 possibili chiavi.

Spazio delle chiavi

Spazio delle chiavi: insieme di tutte le possibili chiavi in un sistema di crittografia.

Nel cifrario di Cesare, utilizzato su testi US-ASCII, posso considerare come spazio delle chiavi I numeri interi da 0 a 127, per un totale di 128 possibili chiavi.

Evito di considerare le chiavi maggiori di 127 perchè cifratura e decifrazione operano modulo 128, per cui, ad esempio

$$\text{cif}(126,37)=(126+37) \bmod 128=163 \bmod 128=\mathbf{35}$$

$$\text{cif}(126,37+128)=(126+37+128) \bmod 128=290 \bmod 128=\mathbf{35}$$

Attacco a forza bruta

Obiettivo: dato un crittotesto C trovare il testo in chiaro T corrispondente tale che $\text{cif}(T,k)=C$ per qualche k .

In un attacco **a forza bruta**, l'attaccante prova a decifrare il crittotesto con **tutte** le chiavi nello spazio delle chiavi.

Attacco a forza bruta

Obiettivo: dato un crittotesto C trovare il testo in chiaro T corrispondente tale che $\text{cif}(T,k)=C$ per qualche k .

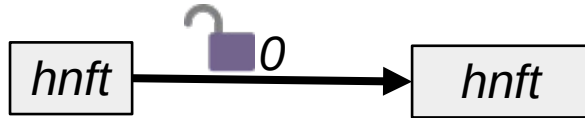
In un attacco **a forza bruta**, l'attaccante prova a decifrare il crittotesto con **tutte** le chiavi nello spazio delle chiavi.

È necessario prima definire un **test** per verificare se la decifrazione con una certa chiave produce come risultato un testo in chiaro *plausibile*. Un esempio di test potrebbe essere

“Il testo in chiaro contiene almeno una parola in lingua italiana.”

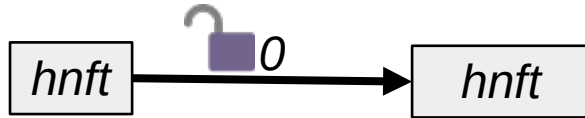
Attacco a forza bruta sul cifrario di Cesare

L'attaccante intercetta il crittogramma "hnft" e vuole scoprire il testo in chiaro.



Attacco a forza bruta sul cifrario di Cesare

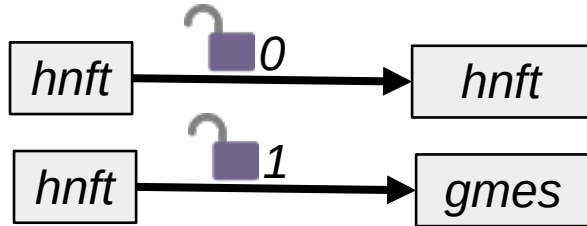
L'attaccante intercetta il crittotesto "hnft" e vuole scoprire il testo in chiaro.



Contiene una parola della lingua italiana? NO

Attacco a forza bruta sul cifrario di Cesare

L'attaccante intercetta il crittogramma "hnft" e vuole scoprire il testo in chiaro.

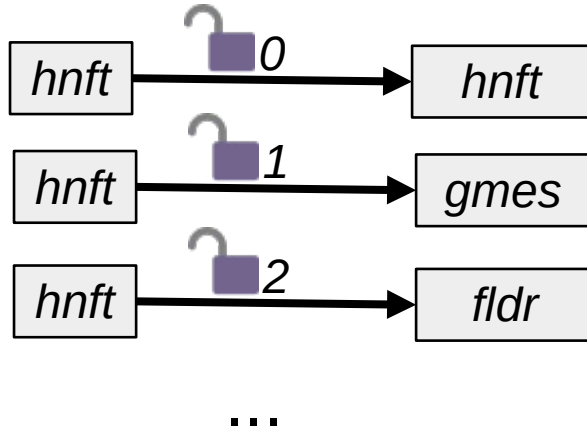


Contiene una parola della lingua italiana? NO

Contiene una parola della lingua italiana? NO

Attacco a forza bruta sul cifrario di Cesare

L'attaccante intercetta il crittogramma "hnft" e vuole scoprire il testo in chiaro.



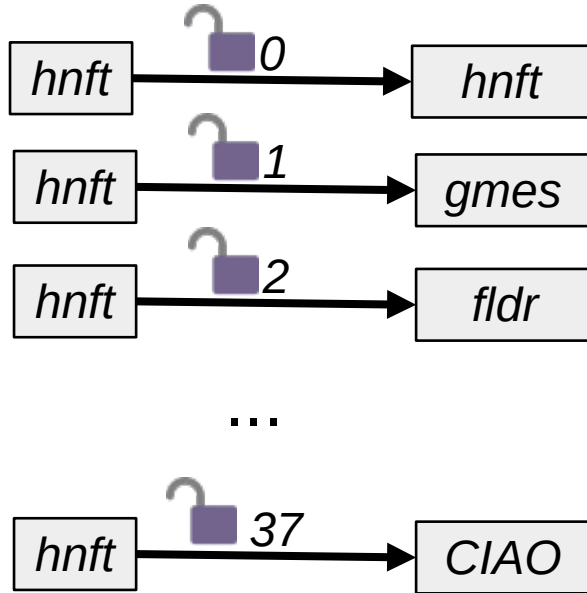
Contiene una parola della lingua italiana? NO

Contiene una parola della lingua italiana? NO

Contiene una parola della lingua italiana? NO

Attacco a forza bruta sul cifrario di Cesare

L'attaccante intercetta il crittogramma "hnft" e vuole scoprire il testo in chiaro.



Contiene una parola della lingua italiana? NO

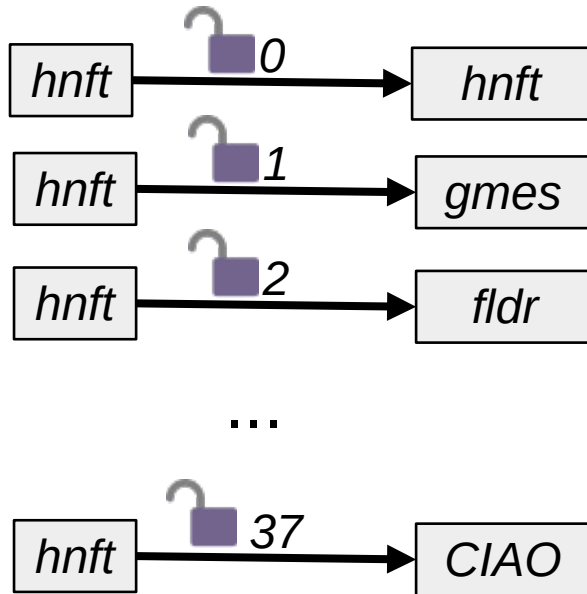
Contiene una parola della lingua italiana? NO

Contiene una parola della lingua italiana? NO

Contiene una parola della lingua italiana? SI.

Attacco a forza bruta sul cifrario di Cesare

L'attaccante intercetta il crittotesto "hnft" e vuole scoprire il testo in chiaro.



Contiene una parola della lingua italiana? NO

Contiene una parola della lingua italiana? NO

Contiene una parola della lingua italiana? NO

Contiene una parola della lingua italiana? SI.

Il testo in chiaro è "**CIAO**" e la chiave è **37**.

Analisi delle frequenze

IX Secolo – Nel *Manoscritto sulla decifrazione dei messaggi crittati* l'autore Abū Yūsuf Ya'qūb ibn Ishāq al-Kindī presenta una tecnica denominata **analisi delle frequenze**.

Se conosco la lingua in cui è scritto il testo in chiaro, posso supporre che la lettera che compare con maggiore frequenza nel testo cifrato corrisponda alla lettera più frequentemente utilizzata in quella lingua.



Analisi delle frequenze - esempio

Dato un crittotesto cifrato con cifrario di Cesare e che deriva da un testo in chiaro in italiano

```
QHOPHCCRGHOFDPPLQ  
GLQRVWUDYLWDPLULW  
URYDLSSHUXQDVHOYDR  
VFXUDFKODGLULWWDY  
LDHUDVPDUULWD
```

Analisi delle frequenze - esempio

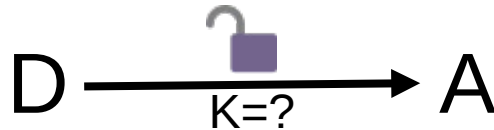
Dato un crittotesto cifrato con cifrario di Cesare e che deriva da un testo in chiaro in italiano. Il carattere che compare più di frequente nel testo cifrato

QHOPHCCRGHOF**D**PPLQ
GLQRVWUD**D**YLW**D**PLULW
URY**D**LSHUXQ**D**VHOY**D**R
VFXU**D**FKOD**D**GLULW**D**Y
L**D**HU**D**VP**D**UULW**D**

Carattere	Frequenza
D	13
L	10
U	9
...	...

Analisi delle frequenze - esempio

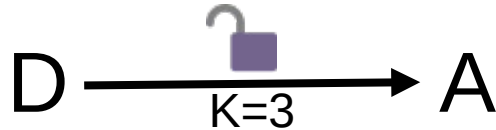
Dato un crittotesto cifrato con cifrario di Cesare e che deriva da un testo in chiaro in italiano. Il carattere che compare più di frequente nel testo cifrato probabilmente corrisponde alla lettera usata più di frequente in italiano: 'A'.



QHOPHCCRGHOFDPPLQ
GLQRVWUDYLWDPLULW
URYDLSSHUXQDVHOYDR
VFXUDFKODGLULWWDY
LDHUDVPDUULWD

Analisi delle frequenze - esempio

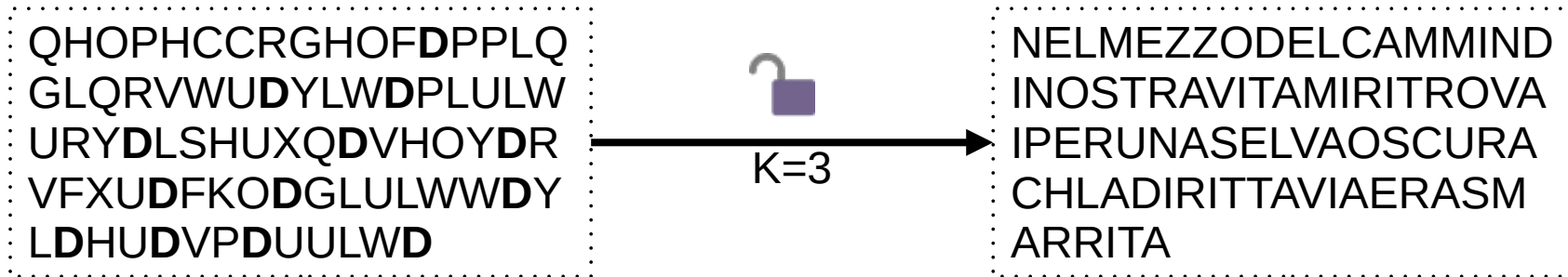
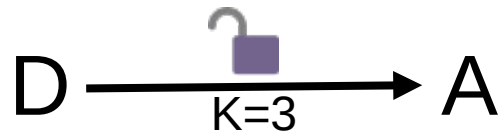
Dato un crittotesto cifrato con cifrario di Cesare e che deriva da un testo in chiaro in italiano. Il carattere che compare più di frequente nel testo cifrato probabilmente corrisponde alla lettera usata più di frequente in italiano: 'A'. Posso quindi calcolare la chiave



QHOPHCCRGHOFDPPLQ
GLQRVWUDYLWDPLULW
URYDLSSHUXQDVHOYDR
VFXUDFKODGLULWWDY
LDHUDVPDUULWD

Analisi delle frequenze - esempio

Dato un crittotesto cifrato con cifrario di Cesare e che deriva da un testo in chiaro in italiano. Il carattere che compare più di frequente nel testo cifrato probabilmente corrisponde alla lettera usata più di frequente in italiano: 'A'. Posso quindi calcolare la chiave e verificare questa ipotesi.



Cifrario di Vigenère

1856 – il **cifrario di Vigenère** utilizza come chiavi sequeze di interi di lunghezza fissa.

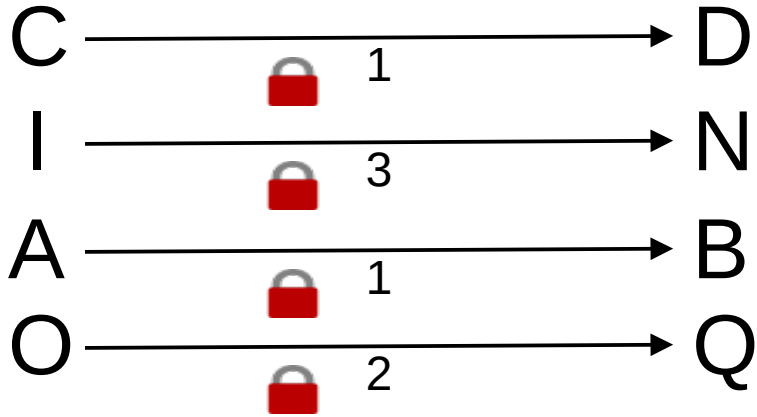
Esempio di chiave di lunghezza 4: (1,3,1,2)

Cifrario di Vigenère

1856 – il **cifrario di Vigenère** utilizza come chiavi sequeze di interi di lunghezza fissa.

Esempio di chiave di lunghezza 4: (1,3,1,2)

Le operazioni di cifratura e la decifrazione dei singoli caratteri coincidono con quelle del cifrario di Cesare, ma il numero utilizzato come chiave dipende dalla posizione del carattere: il primo carattere sarà cifrato col primo elemento della chiave, il secondo col secondo, e così via.



Cifrario di Vigenère

1856 – il **cifrario di Vigenère** utilizza come chiavi sequeze di interi di lunghezza fissa.

Esempio di chiave di lunghezza 4: (1,3,1,2)

Le operazioni di cifratura e la decifrazione dei singoli caratteri coincidono con quelle del cifrario di Cesare, ma il numero utilizzato come chiave dipende dalla posizione del carattere: il primo carattere sarà cifrato col primo elemento della chiave, il secondo col secondo, e così via.

Nel caso in cui la lunghezza del messaggio ecceda quella della chiave, è necessario ripetere la chiave.

Testo in chiaro	A	C	Q	U	I	L	A	
Chiave	1	3	1	2	1	3	1	2
Crittotesto	B	F	R	W	J	O	B	

Crittografia Perfetta

1917 – il **cifrario di Vernam** usa il cifrario di Vigenère ma impone

- che si utilizzino chiavi della stessa lunghezza del testo in chiaro e

Crittografia Perfetta

1917 – il **cifrario di Vernam** usa il cifrario di Vigenère ma impone

- che si utilizzino chiavi della stessa lunghezza del testo in chiaro e
- che ogni chiave sia utilizzata un'unica volta (One Time Pad).

Crittografia Perfetta

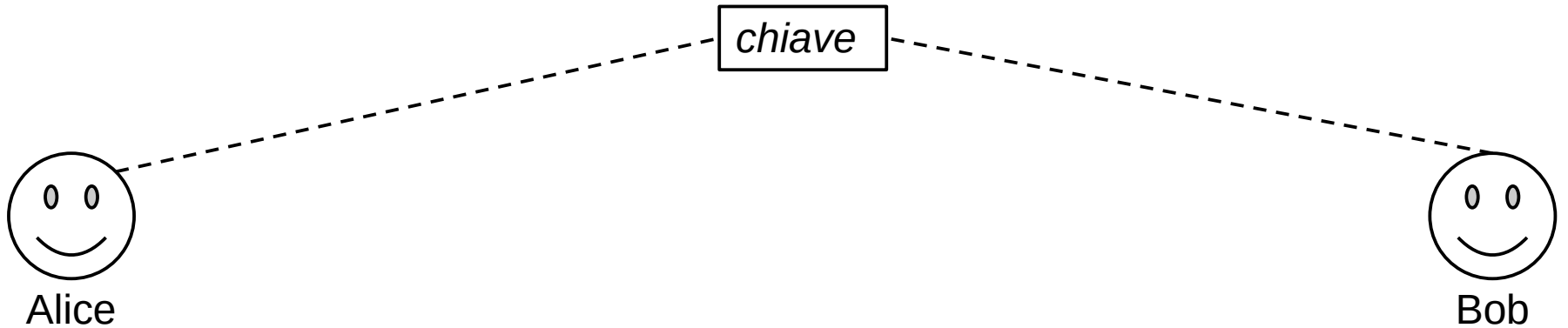
1917 – il **cifrario di Vernam** usa il cifrario di Vigenère ma impone

- che si utilizzino chiavi della stessa lunghezza del testo in chiaro e
- che ogni chiave sia utilizzata un'unica volta (One Time Pad).

Può essere forzato solo utilizzando attacchi a forza bruta.

Scambiarsi le chiavi

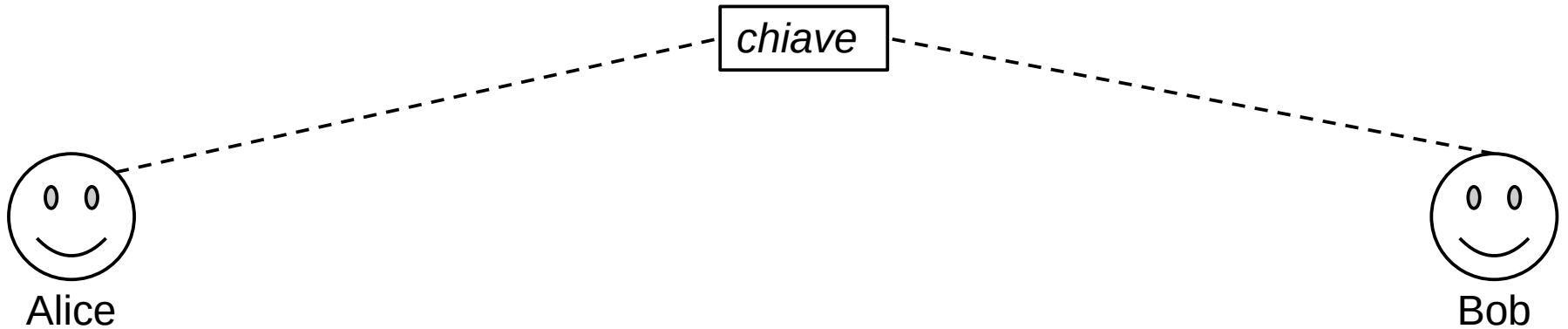
Le tecniche di **crittografia simmetrica** si basano sulla condivisione di un segreto, detto **chiave**. tra le parti che devono scambiarsi messaggi confidenziali.



Scambiarsi le chiavi

Le tecniche di **crittografia simmetrica** si basano sulla condivisione di un segreto, detto **chiave**. tra le parti che devono scambiarsi messaggi confidenziali.

È necessario che la condivisione avvenga in maniera sicura



Crittografia asimmetrica

Le tecniche di **crittografia simmetrica** si basano sulla condivisione di un segreto, detto **chiave**. tra le parti che devono scambiarsi messaggi confidenziali.

È necessario che la condivisione avvenga in maniera sicura, solitamente di persona.

