COESIONE ITALIA 21-27 PIEMONTE
Cofinanziato dall'Unione europea
REGIONE PIEMONTE

DIFFIE-HELLMAN KEY EXCHANGE

Sicurezza informatica

Elena Maria Dal Santo

elenamaria.dalsanto@its-ictpiemonte.it

Intervento realizzato da
ITS TECNOLOGIE DELL'INFORMAZIONE E DELLA COMUNICAZIONE

Hai letto il mio messaggio?

La chiave deve essere CONDIVISA!

Non posso! Non hai condiviso la CHIAVE!

Proprietà delle chiavi crittografiche

Casuale

Protetta

Condivisa

Proprietà delle chiavi crittografiche

La potenza di un sistema crittografico dipende dalla tecnica usata per condividere la chiave.

Lo SCAMBIO DELLE CHIAVI è un problema.

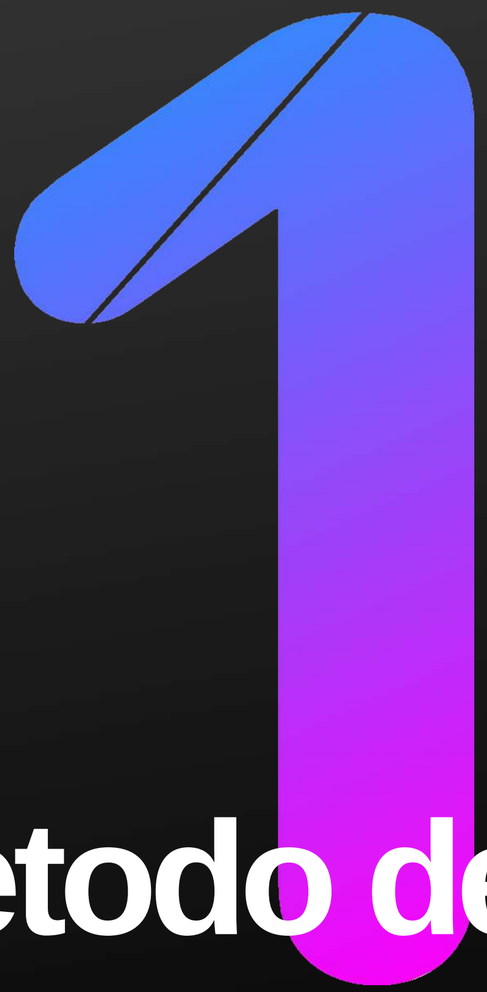
Come si può condividere la chiave?

A mano

Terza parte

Canale sicuro

I primi due metodi non sono utilizzabili in epoca informatica; il terzo presuppone che una chiave sia già stata scambiata.



Il metodo del doppio lucchetto

Metodo del doppio lucchetto

Metodo del doppio lucchetto

Metodo del doppio lucchetto

Metodo del doppio lucchetto

Metodo del doppio lucchetto

Metodo del doppio lucchetto

Metodo del doppio lucchetto

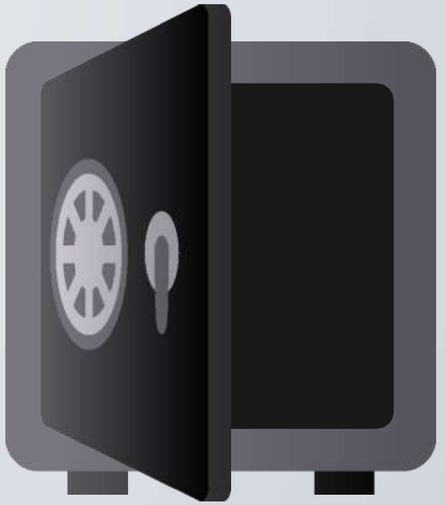
Metodo del doppio lucchetto

Metodo del doppio lucchetto

Metodo del doppio lucchetto

Metodo del doppio lucchetto

Perché questo metodo non può funzionare?



Inoltre, col metodo del doppio lucchetto, il messaggio fa avanti e indietro ben 3 volte sullo stesso canale!

Può essere oggetto di un'analisi differenziale

Attacco che prevede lo studio del testo dopo ogni rimpallo in cerca di eventuali ripetizioni/indizi per costruire un metodo di decifrazione

Composizione di cifrature

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

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

Messaggio	ci vediamo all una
Cifrato da Bob	MJ ZAGJCIB CWW SQB
Cifrato da Alice	YD ZHADSVF SII WNF
Decifrato da Bob	RV WSEVUZK UMM LGK
Decifrato da Alice	vi sckidyh dxx zeh

Composizione di cifrature

Cos’è successo?

Cambiamo un secondo notazione…

m	messaggio
A(m)	chiave di cifratura di Alice
$A^{-1}(m)$	chiave di decifratura di Alice
B(m)	chiave di cifratura del Bianconiglio
$B^{-1}(m)$	chiave di decifratura del Bianconiglio

Cos’è successo?

Quello che abbiamo appena fatto potrebbe essere riscritto come

$B^{-1}(A^{-1}(B(A(m))$

$$\frac{1}{B}\left(\frac{1}{A}\left(B\left(A(m)\right)\right)\right.$$

Posso semplificare come facevo alle superiori!

Purtroppo, non sempre è possibile farlo!

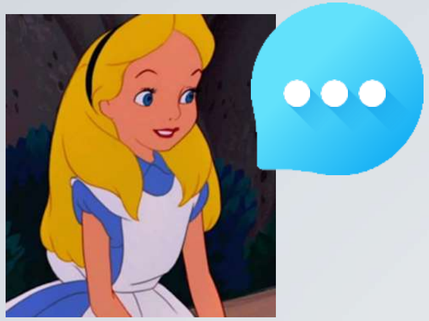
Cos’è successo?

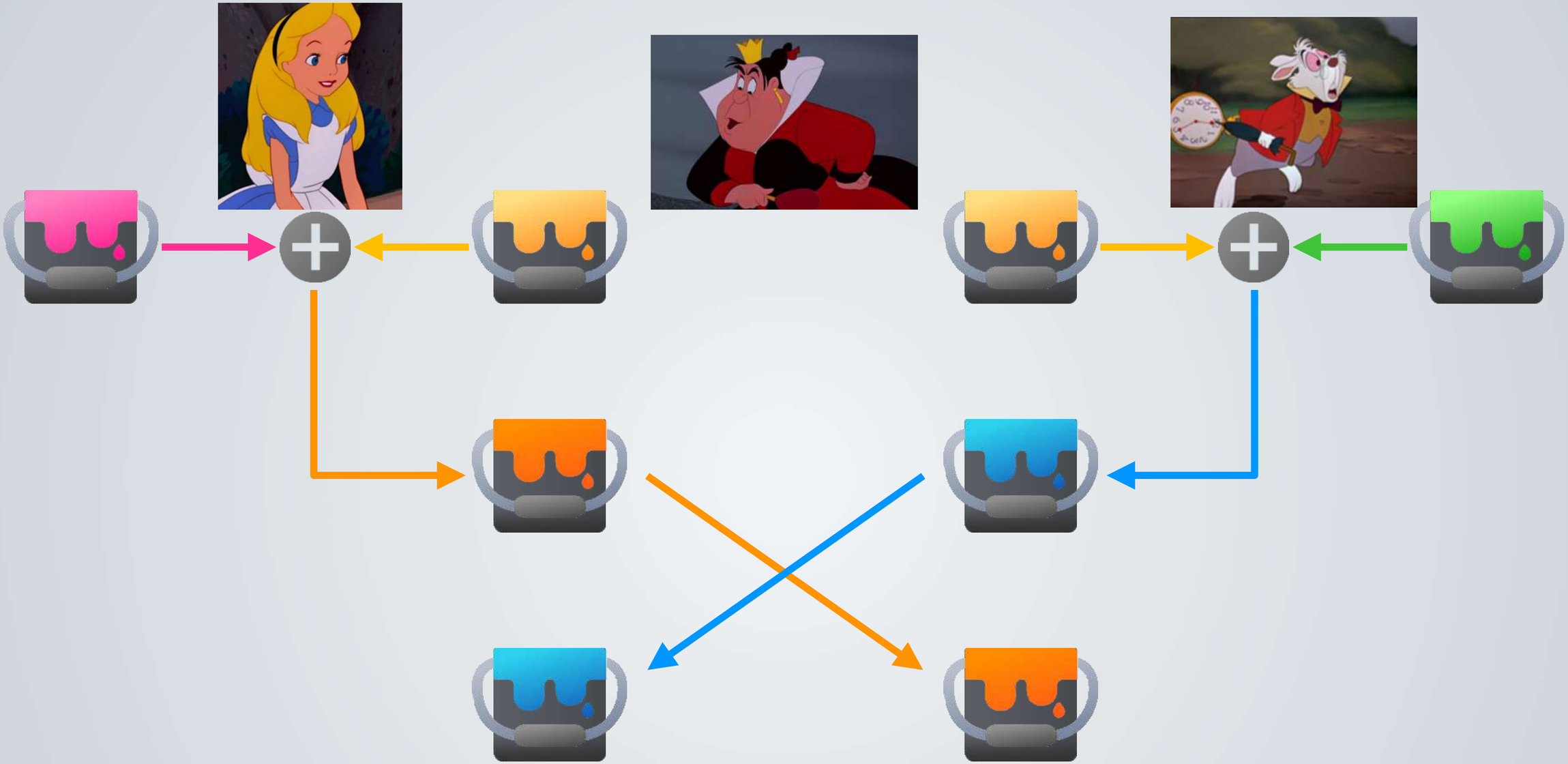
Solo per cifrari a trasposizione (es. atbash, Giulio Cesare) o cifrari monoalfabetici posso ‘’semplificare’’

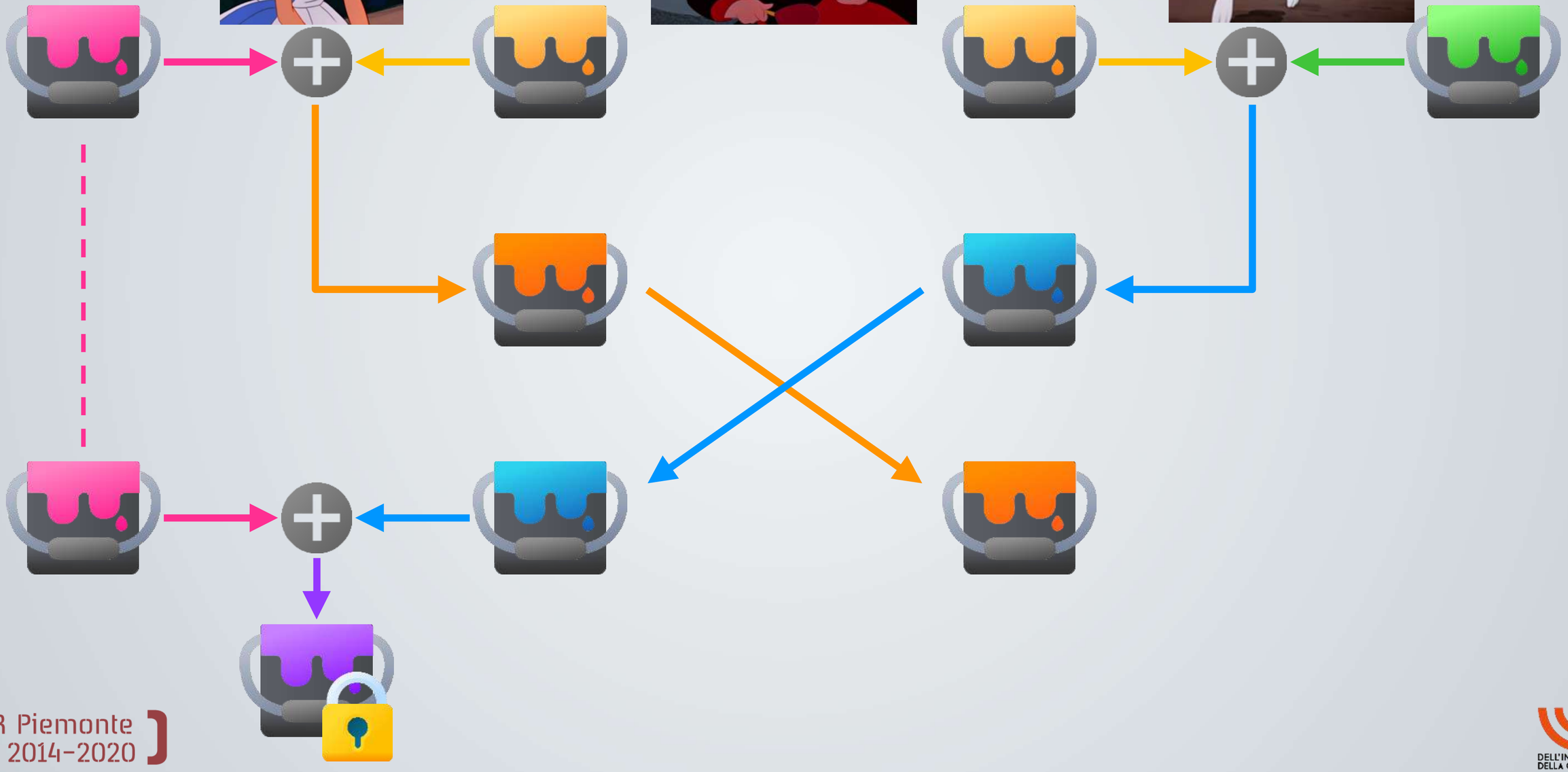
Il metodo dei colori

2

Lo scambio delle chiavi di Diffie-Hellman







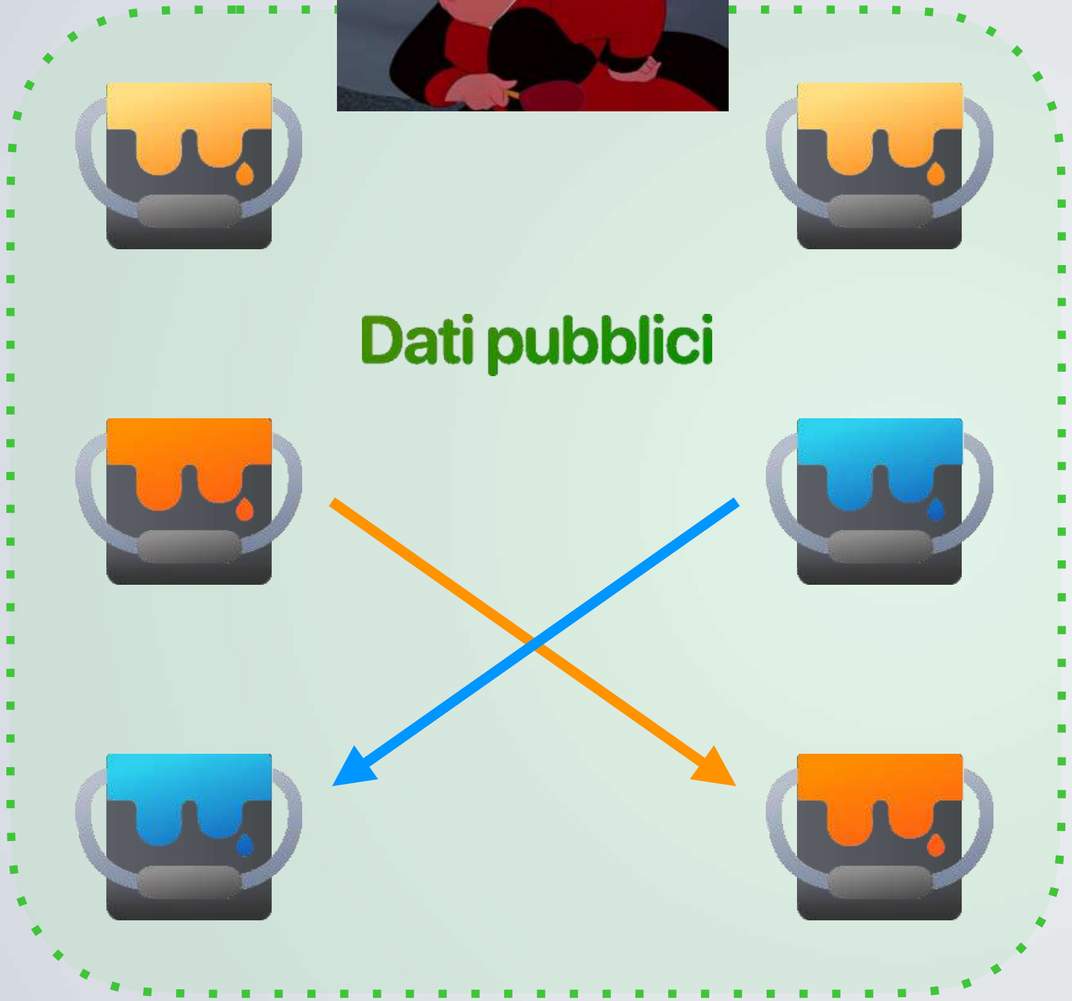
Chiave segreta condivisa

Dati pubblici

Chiave segreta condivisa

Dati pubblici

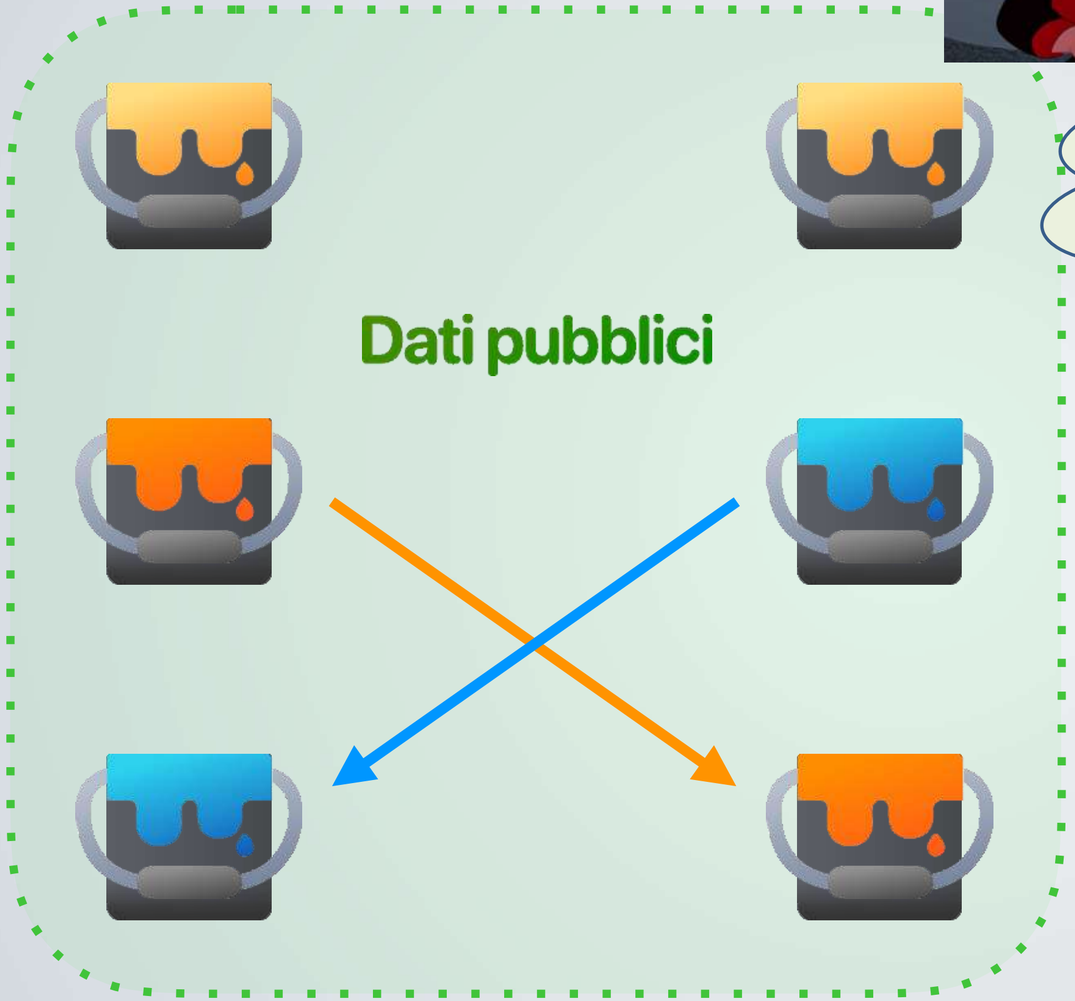
Chiave segreta condivisa



Ci sono infiniti colori!

Difficilmente E potrà arrivare a quello scelto!

Se usate colori così semplici, con qualche tentativo riuscirò a trovare la chiave!



Perché la procedura è sicura?

Perché nelle implementazioni reali si usano numeri di

300

cifre

Perché la procedura è sicura?

I numeri usati, inoltre, non sono ovviamente inviati ‘’così come sono”, ma vengono sfruttate funzioni matematiche quali il modulo e il problema del logaritmo discreto…

Ci interessano queste funzioni?


NO.
Ha ragione!
Ci interessa capire pochi concetti base...

Siamo su un canale di comunicazione insicuro!

Non ci siamo mai parlati prima d’ora!

EPPURE

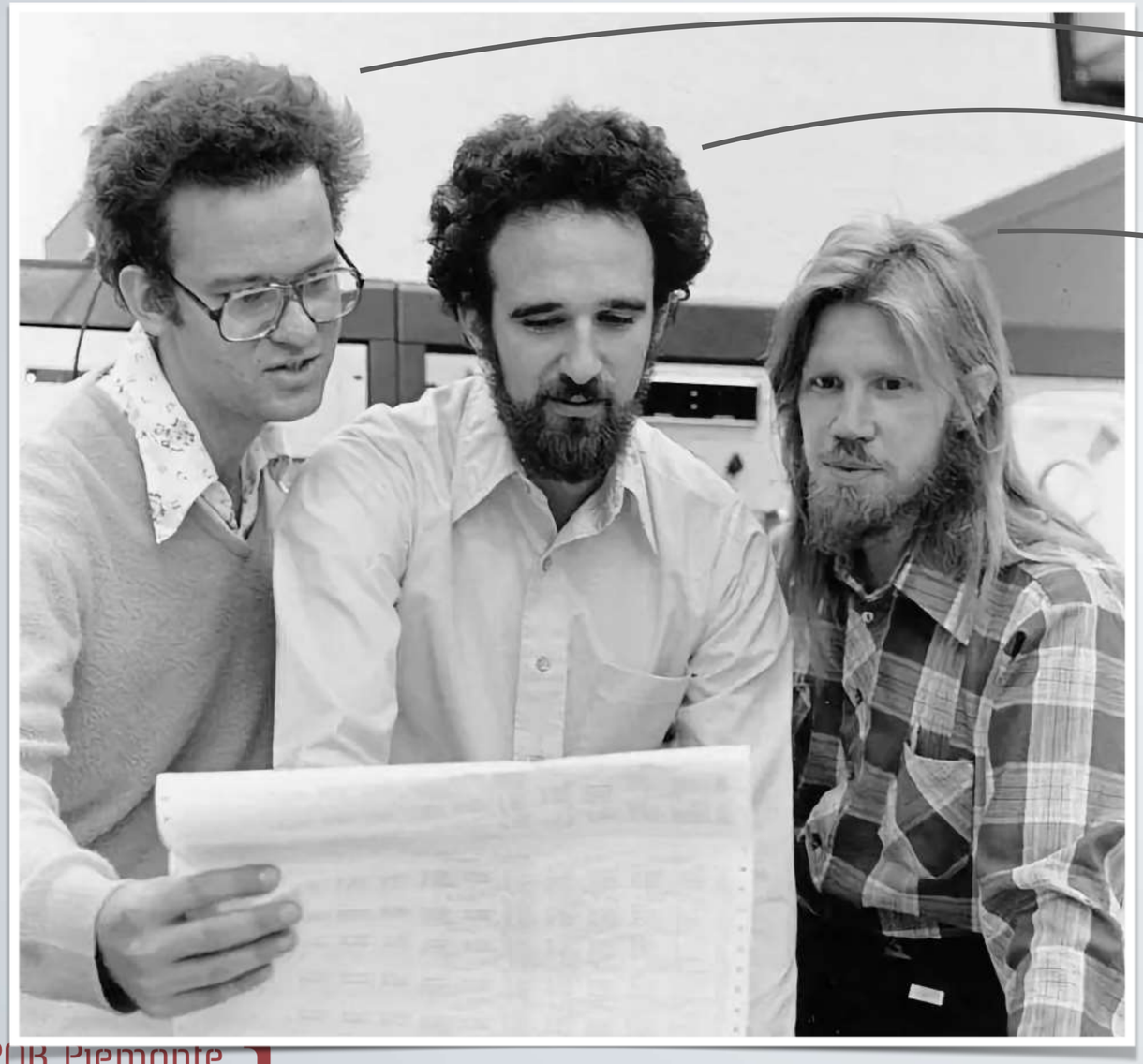
A e B sono riusciti a stabilire una chiave

- condivisa
- Segreta

Le funzioni usate nell’implementazione “reale” sono computazionalmente molto pesanti, soprattutto se implicano numeri grandi.

È un algoritmo che si può rompere, ma richiederebbe un tempo potenzialmente infinito!

Diffie, Hellman e Merkle



Ralph Merkle

Martin Hellman

Whitfield Diffie

Risolvono il problema dello scambio delle chiavi nel 1976.

È il primo metodo pratico per scambiare chiavi crittografiche in un canale insicuro ed è tutt'oggi comunemente usato.

Man-in-the-middle attack

Man-in-the-middle attack

A e il B devono scambiarsi l'informazione pubblica.

E controlla il canale di comunicazione.

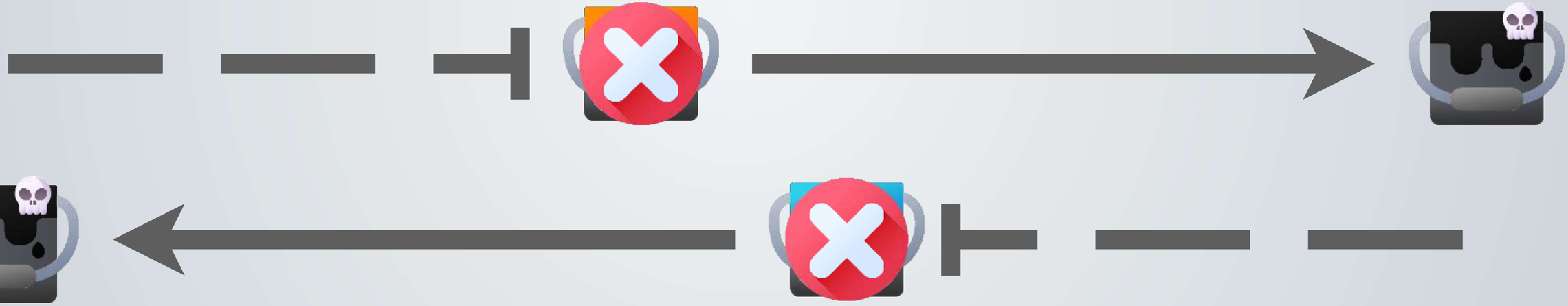
Man-in-the-middle attack

A e B inviano l'informazione, ma E le intercetta.

Man-in-the-middle attack

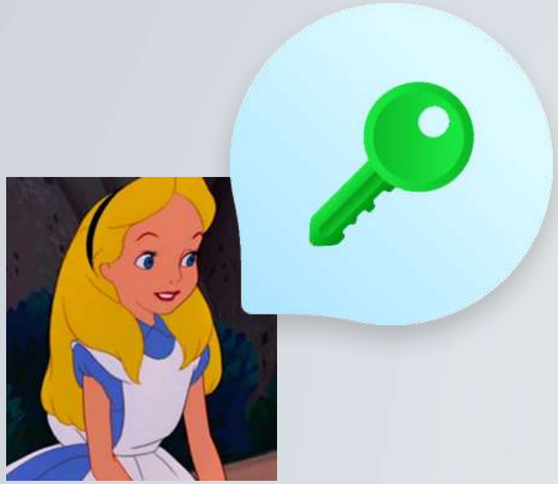
E crea delle versioni fraudolente delle informazioni pubbliche di A e B.

Man-in-the-middle attack



Eve spedisce le versioni fraudolente ingannando entrambi.

Man-in-the-middle attack



Expectation

Reality

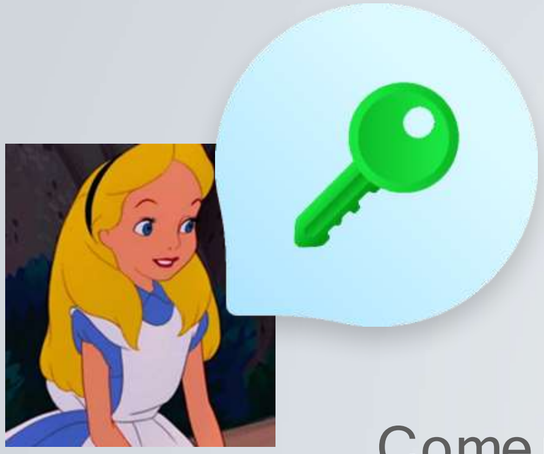
Comunicazione cifrata

Intercettazione

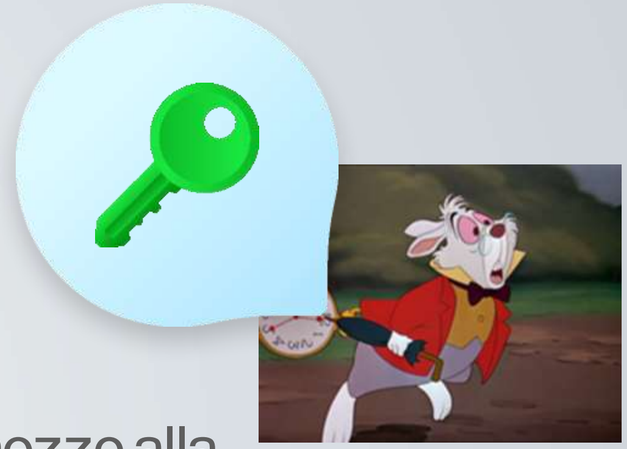
Comunicazione cifrata

A e B credono di aver condiviso una chiave, ma l'hanno in realtà condivisa con E, che ora sta in mezzo alla conversazione e può intercettare tutto.

Risolvere il Man-in-the-middle



Canale



Come possiamo verificare che nessuno si sia messo in mezzo alla comunicazione?

Verifica manuale

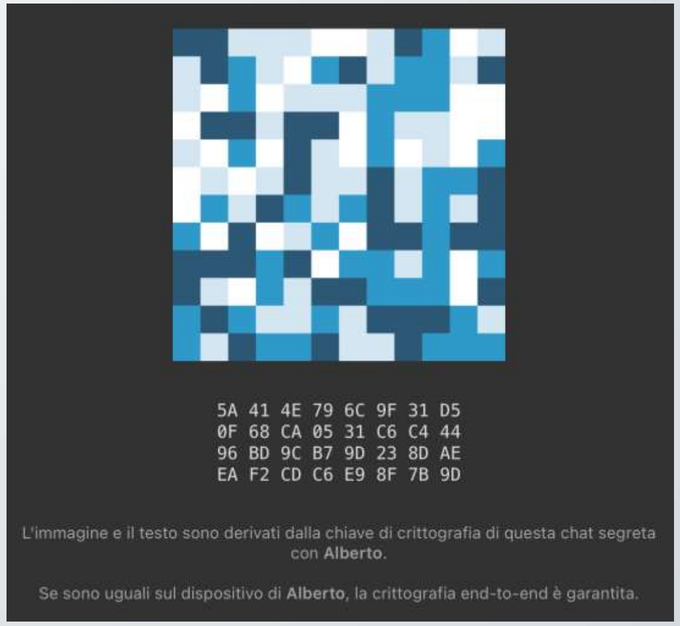
Certificazione

(le vedremo più avanti…)

Quindi nel mondo reale si usa DH?

La crittografia end-to-end

"Keys for end-to-end encrypted calls and chats are generated using the Diffie-Hellman key exchange. Users who are on a call/chat can ensure that there is no Man in the Middle by comparing key visualizations."



Quindi nel mondo reale si usa DH?