Protocolli esoterici

Roberto Qiu, Federico Violante,
Simone Coccia, Stefano Limiti

Avvertenze: tutti gli esempi usati sono tratti dal libro di Schneier e, esclusi alcuni nomi di persona, non sono frutto di strane fantasie personali.

Anonimous Message Broadcasting

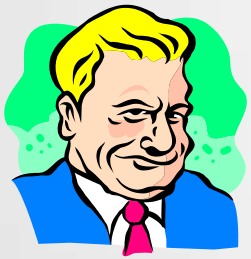
Roberto Qiu

- E’ un protocollo che permette di mandare messaggi broadcast in maniera del tutto anonima.

- Presentiamo l’algoritmo con un semplice esempio, proposto da David Chaum:

The Dining Cryptographers Problem

A cena con crittografi...

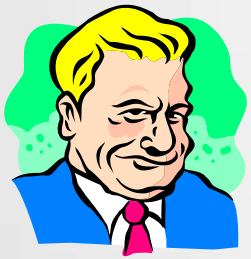


Bob

Alice

Carol

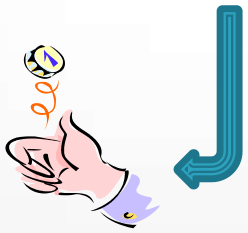
A cena con crittografi...



Bob

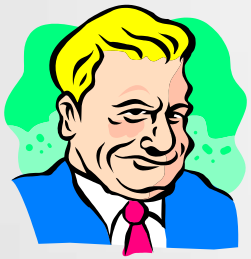
#different = 0
#same = 0

Alice



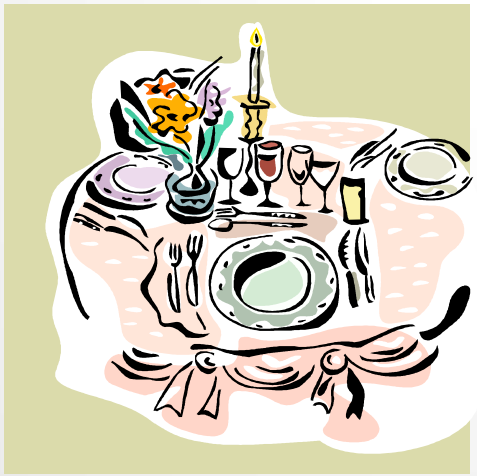
Carol

A cena con crittografi...



Bob

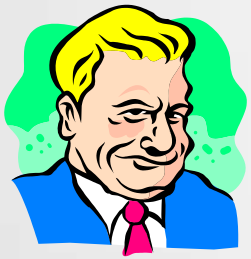
#different = 0
#same = 0



Alice

Carol

A cena con crittografi...



Bob

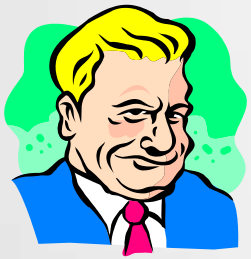
Alice

Carol

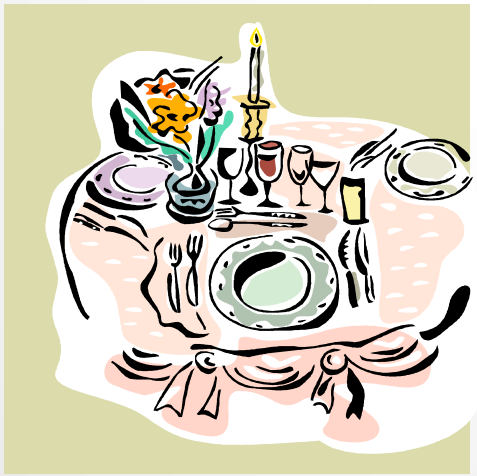
#different = 0
#same = 0

A cena con crittografi...

Different!



Bob

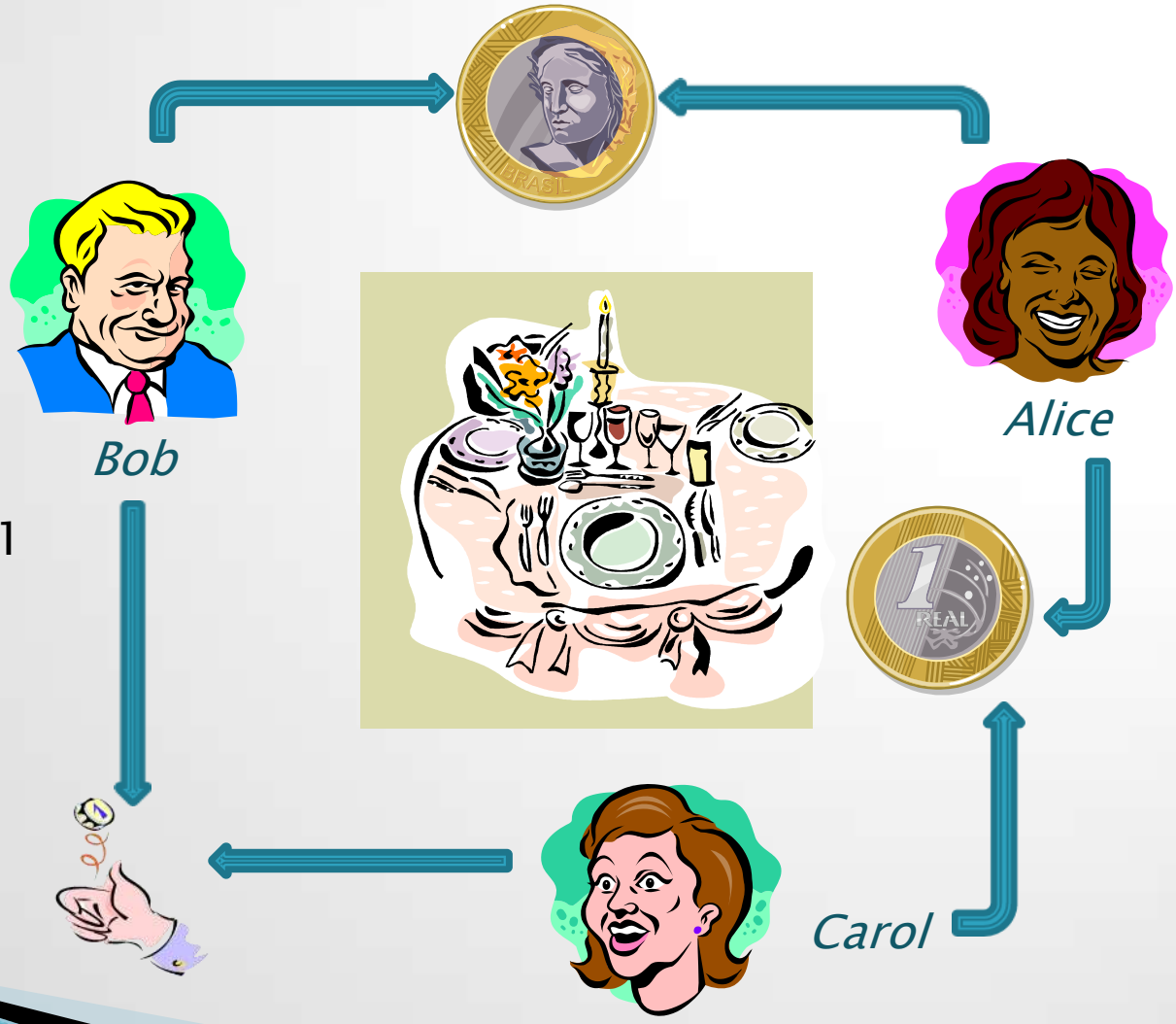


Alice

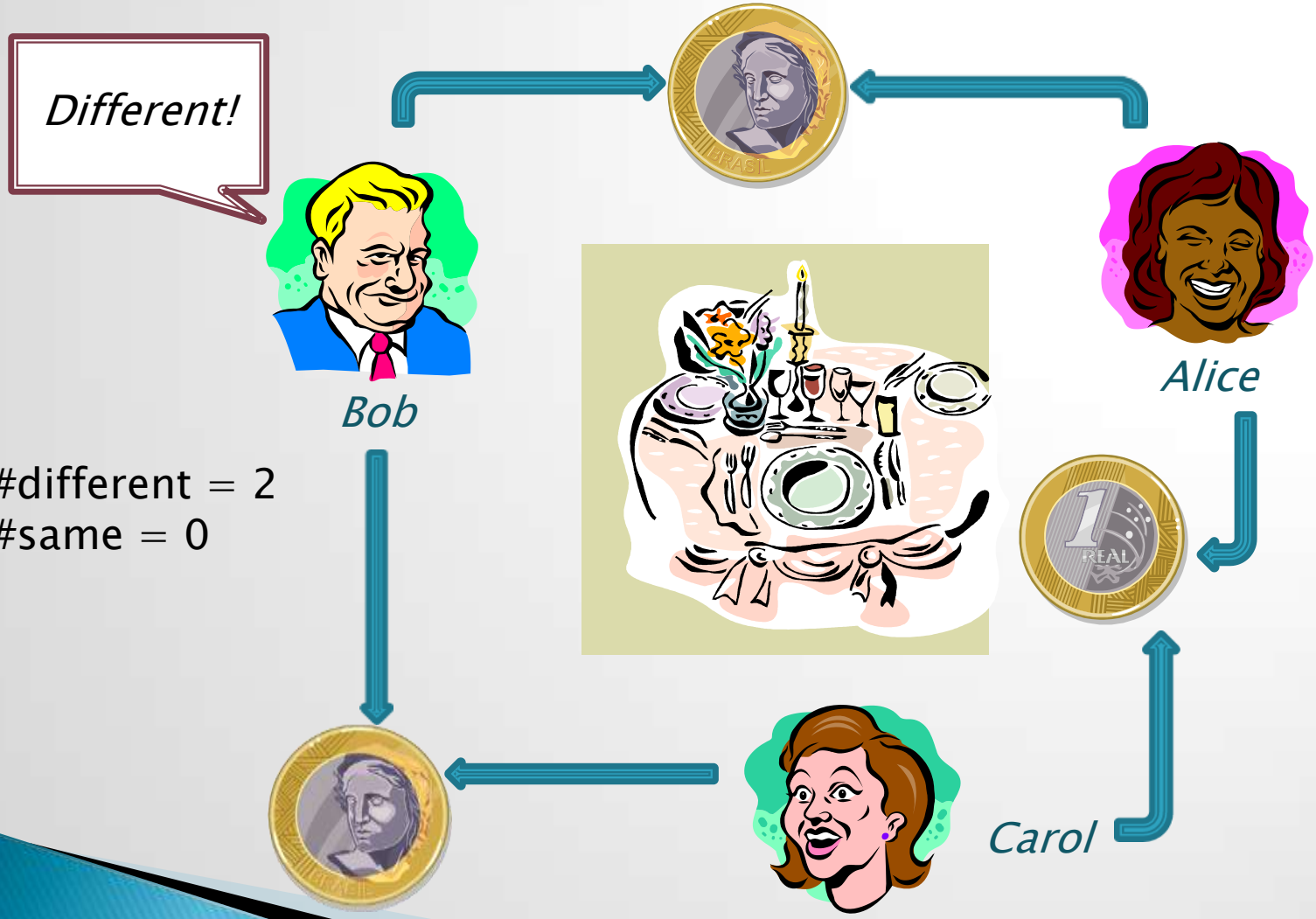
#different = 1
#same = 0

Carol

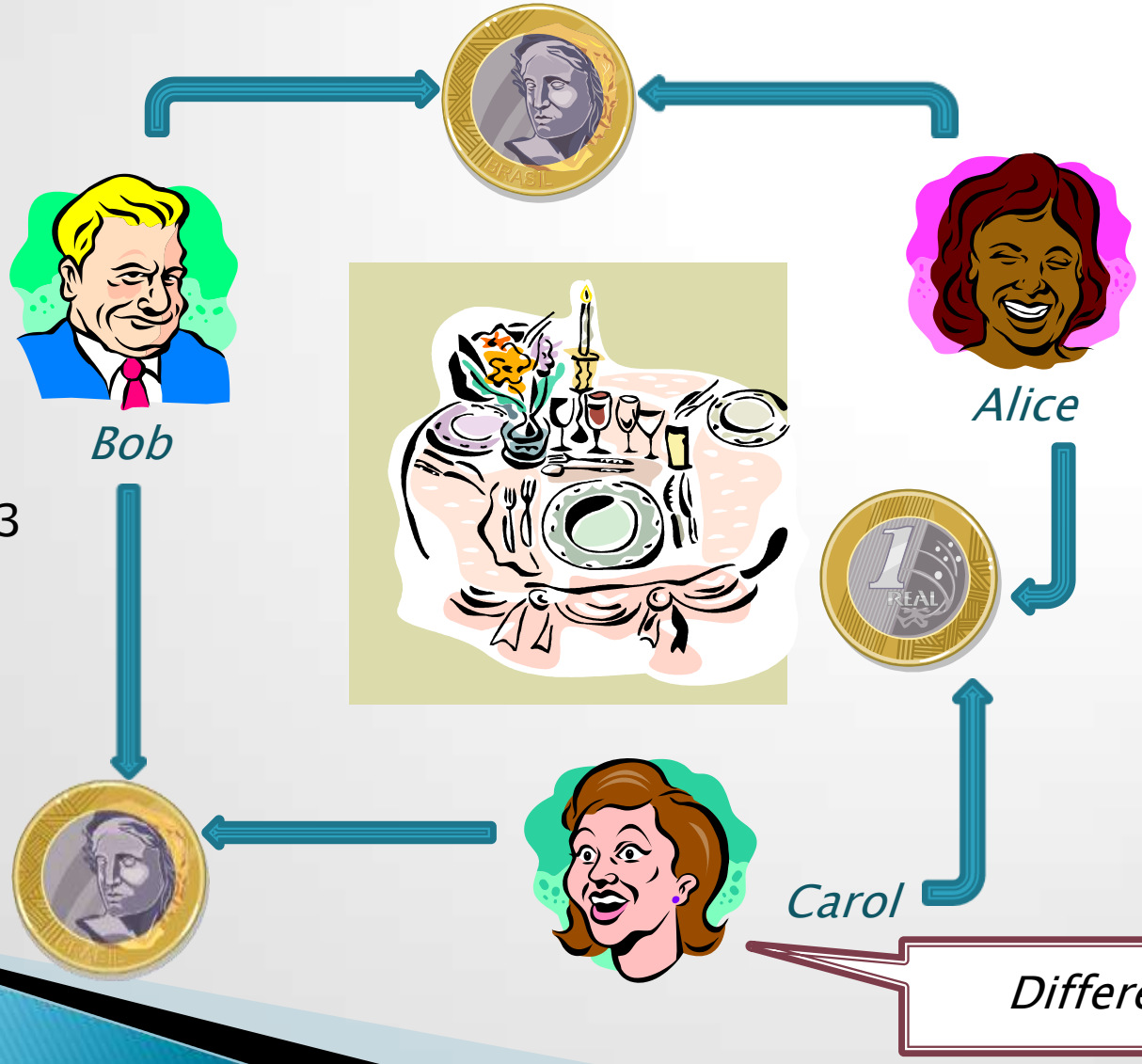
A cena con crittografi...



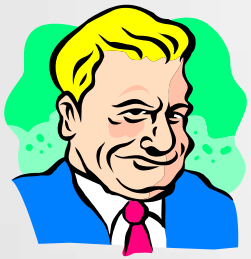
A cena con crittografi...



A cena con crittografi...

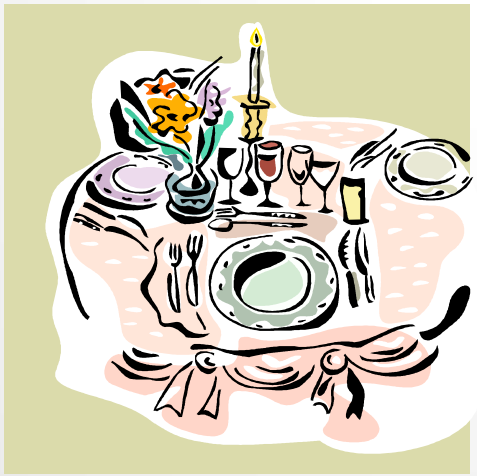


A cena con crittografi...



Bob

Alice



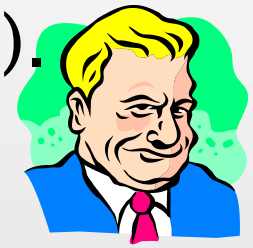
#different = 3
#same = 0

Carol

dispari di Different... Qualcuno ha pagato la cena!

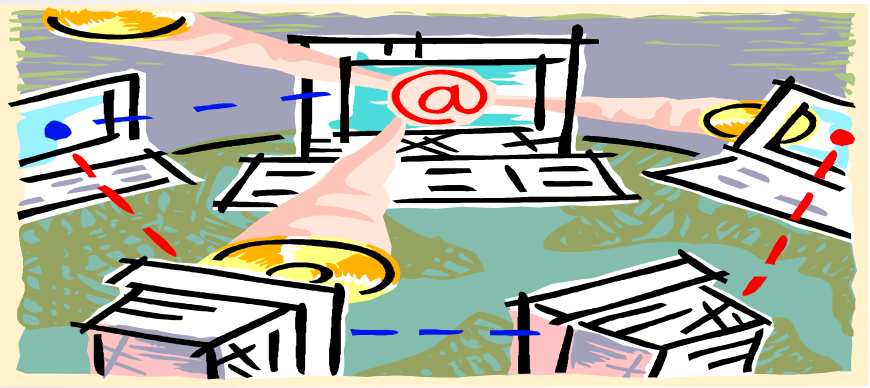
A cena con crittografi...

Bob ha pagato la cena in quanto ha detto l'opposto dell'esito dei lanci a cui ha assistito; tuttavia né Alice né Carol hanno modo di sapere con esattezza chi abbia pagato tra i due commensali che ognuna ha di fronte (escludendo se stessi).



Generalizzando...

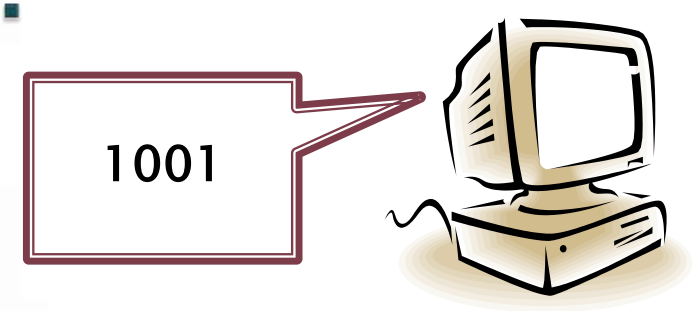
L'algoritmo può essere esteso a *n* persone disposte in circolo che a due a due si lanciano la monetina

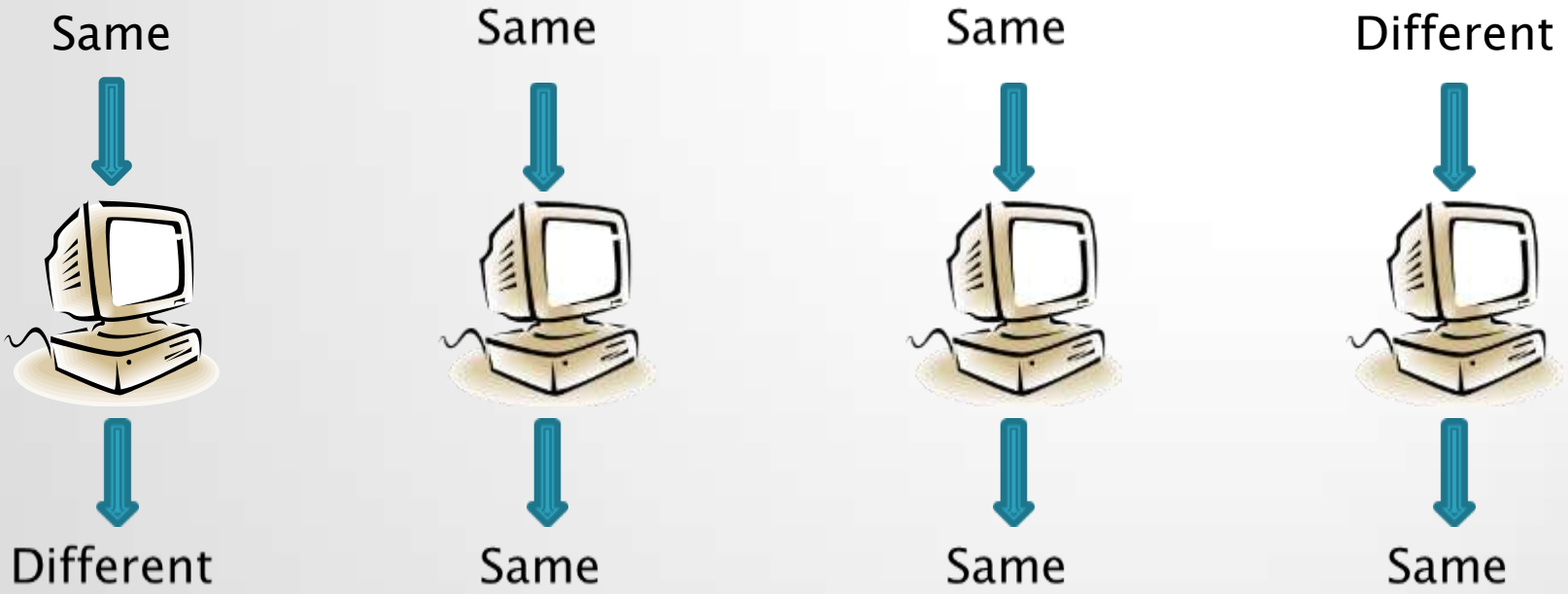


E' applicabile in una rete di utenti connessi in circolo. Al lancio della moneta è sostituita una funzione che non può essere compresa al di fuori della coppia che sta comunicando.

Generalizzando...

Stringa da trasmettere:





Blind Signature

- Protocollo usato se non si vuole far conoscere il contenuto di un documento a chi deve firmarlo.
- Molto usato in ambito di e-voting ed e-cash.
- Un primo protocollo molto semplice:

The Completely Blind Signature

I passi

- (1) Alice moltiplica il documento da firmare con un valore random (blinding factor);
- (2) Alice spedisce il documento a Bob;
- (3) Bob firma il documento;
- (4) Alice divide il documento per il blinding factor ed ottiene il documento originale firmato.

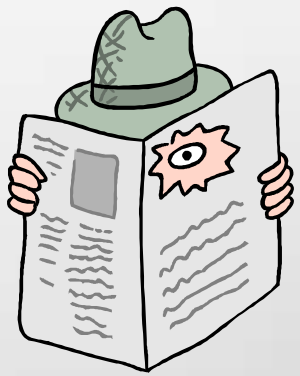
Considerazioni...

- La firma e la moltiplicazione devono essere commutative.
- Bob non ha modo di imbrogliare in quanto non conosce il contenuto del documento.
- Se il documento è presentato a distanza di tempo Bob riconosce la proprio firma, ma non può risalire a quando lo abbia firmato e in che protocollo.
- Alice, tuttavia, può far firmare a Bob tutto ciò che vuole...

L’agenzia di controspionaggio

Agenti in copertura devono ricevere permessi di immunità diplomatica. Hanno diversi nomi in codice e non vogliono che l’agenzia sia a conoscenza del nome usato per la missione.

D’altronde l’agenzia non è intenzionata a firmare alla «cieca» qualsiasi documento che l’agente le mandi…come la richiesta di una pensione da 10 milioni di dollari!

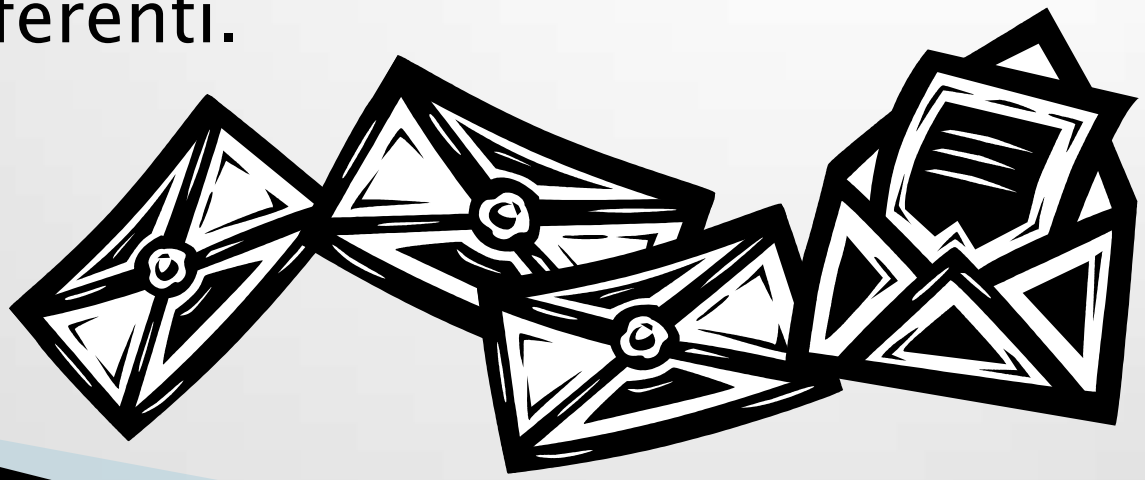


Soluzione

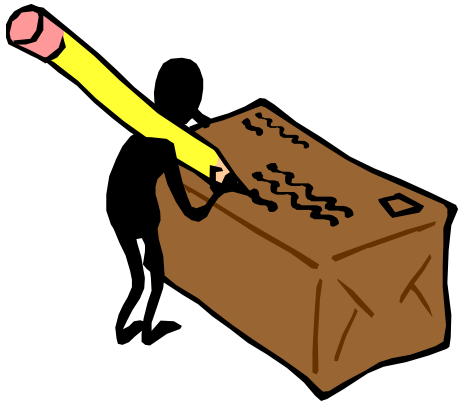
ALICE = Agency's Large Intelligence Computing Engine

BOB = agent in Bogota Operations Branch

- BOB prepara n documenti che gli diano immunità diplomatica, ognuno con nomi in codice differenti.



- BOB nasconde ognuno di questi documenti con un blinding factor differente



- BOB spedisce tutti gli n documenti ad ALICE
- ALICE sceglie n-1 documenti a caso e chiede per ognuno il suo blinding factor
- BOB manda ed ALICE i blinding factor richiesti

- ALICE rimuove il blinding factor, apre gli n-1 documenti e verifica che siano corretti (e non pensioni milionarie).

- ALICE firma e spedisce a BOB l'unico documento rimasto chiuso.

- BOB rimuove il blinding factor e legge il suo nuovo nome in codice per la sua missione in Bogota: «Crimson Steak» ovvero «Bistecca Rosso Sangue»!

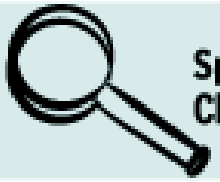
Conclusione

- BOB non può barare in quanto le probabilità sono contro di lui (1/n!).
- ALICE è quindi sicura di poter firmare il documento anche se non ne ha controllato il contenuto.
- Sono mantenute tutte le proprietà di anonimato, desiderate dall'agente.

Votazioni elettroniche sicure

Federico Violante

Dio denaro VS Diritto di voto

	LAS VEGAS SLOTS	ELECTRONIC VOTING MACHINES
Software	State of Nevada has access to all software. Illegal to use software that is not on file.	Software is a trade secret.
 Spot-Checking	State gaming inspectors show up unannounced at casinos to compare computer chips with those on file. If there is a discrepancy, the machine is shut down and investigated.	No checks are required. Election officials have no chip to compare with the one found in the machine.
Background Scrutiny	Manufacturers subjected to background checks. Employees are investigated for criminal records.	Citizens have no way of knowing, for example, whether programmers have been convicted of fraud.
Equipment Certification	By a public agency at arm's length from manufacturers. Public questions invited.	By for-profit companies chosen and paid by the manufacturers. No public information on how the testing is done.
Handling Disputes	Casino must contact the Gaming Control Board, which has investigators on call round the clock. They can open up machines to inspect internal mechanisms and records of recent gambling outcomes.	In most cases, a voter's only recourse is to call a number at the board of elections that may or may not work to lodge a complaint that may or may not be investigated.

Risultato della partita

3 – 0

Dio denaro vince a tavolino per manifesta superiorità

Protocollo ideale

Il protocollo ideale deve garantire almeno questi 6 requisiti:

- 1. Solo gli aventi diritto possono votare.
- 2. Nessuno deve poter votare due volte.
- 3. Nessuno deve poter determinare il voto di qualcun'altro.
- 4. Nessuno deve poter duplicare il voto di qualcun'altro (è il requisito più difficile)
- 5. Nessuno deve poter modificare il voto di qualcun'altro senza essere scoperto.
- 6. Ogni avente diritto deve poter essere sicuro che il suo voto è stato registrato al fine del conteggio.

Protocollo di voto semplicistico #1

- (1) Ogni elettore cripta il suo voto con la chiave pubblica della Central Tabulating Facility (CTF, l'ente che raccoglie tutti i voti elettronici)
- (2) Ogni elettore invia il suo voto alla CTF.
- (3) La CTF decritta i voti, li conteggia e li rende pubblici.

La CTF non sa se hanno votato gli aventi diritto, e quante volte hanno votato ciascuno!

Protocollo di voto semplicistico #2

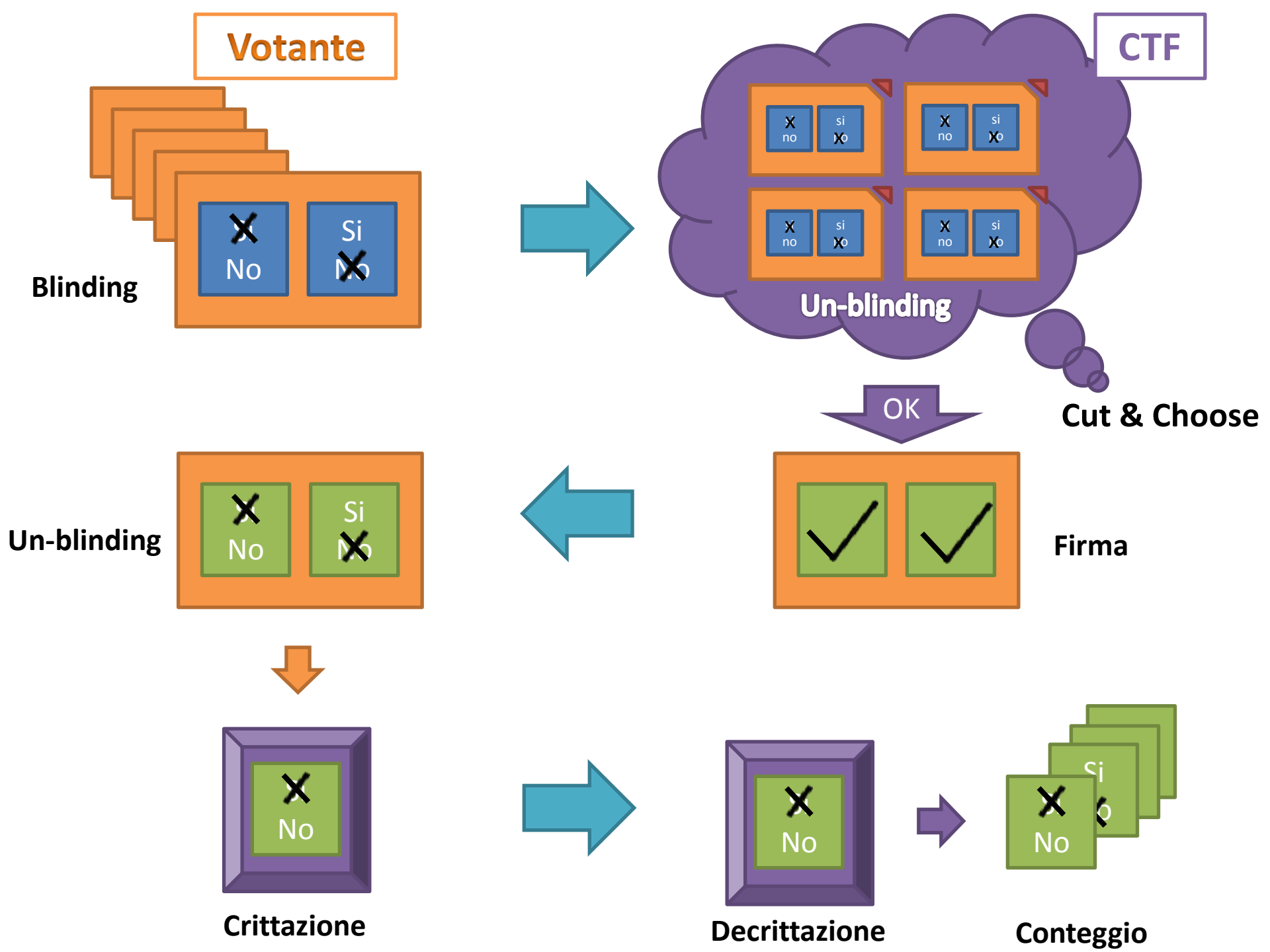
- (0) Ogni elettore firma il suo voto con la propria chiave privata.
- (1) Ogni elettore cripta il suo voto firmato con la chiave pubblica della CTF.
- (2) Ogni elettore invia il suo voto alla CTF.
- (3) La CTF decritta i voti, controlla le firme di ciascuno, conteggia i voti e li rende pubblici.

La CTF conosce i voti di ciascuno!

Voto con Firme Cieche

Vogliamo dissociare il voto dal votante, mantenendo però il controllo sugli aventi diritto.

- Le firme cieche sono la scelta naturale per raggiungere questo obiettivo.


Votante
Blinding
No
Si
CTF
Un-blinding
Cut & Choose
OK
Firma
Un-blinding
Crittazione
Decrittazione
Conteggio

Pro (1)

Un votante malintenzionato non può rompere il sistema e votare più volte perché non può:

- falsificare la firma della CTF sulle schede
- avere più di una scheda validata dal CTF
- modificare i voti degli altri votanti perché criptati

I voti sono quindi unici: ciò è garantito dalla fase di cut-and-choose eseguita dalla CTF.

Pro (2)

Una CTF malintenzionata non può rompere il sistema perché:

- non può conoscere le scelte di voto dei votanti: firma le schede senza conoscere la corrispondenza ID-votante.
- solo il votante può controllare che il suo voto sia stato conteggiato correttamente consultando la corrispondenza ID-voto nella tabella finale

Contro

- Se l'invio della scheda dal votante alla CTF non è anonimo la CTF può registrare il voto dell'elettore.
- Se la CTF cambia il voto di un elettore, questo non ha i mezzi per dimostrarlo.
- La CTF può mettersi nei panni di milioni di votanti inesistenti e generare un grande numero di voti perfettamente validi.

Voto con due CTF

- Si usano una Central Legitimization Agency (CLA) per certificare i voti e una CTF per contarli.
- Nessuna delle due ha i mezzi per truccare le elezioni autonomamente.

Voto con due CTF (1)

- (1) Ogni votante chiede alla CLA un codice di validazione
- (2) La CLA risponde inviando un codice univoco generato in modo random. Registra in due liste tutti i codici usati e tutti i votanti.
- (3) La CLA invia solo la lista dei codici alla CTF.
- (4) Ogni votante sceglie un ID random univoco e lo scrive insieme al codice di validazione e al voto nella scheda che invia alla CTF.

Voto con due CTF (2)

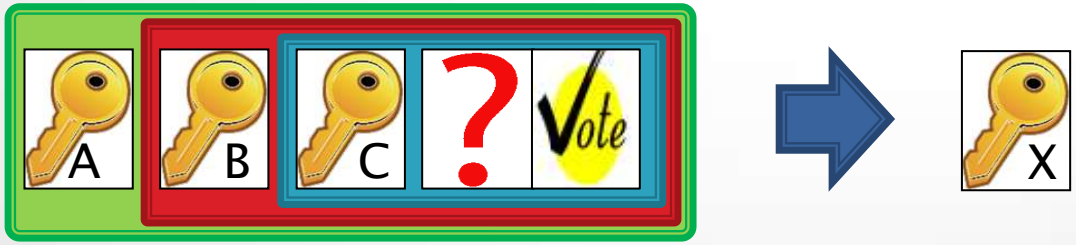
- (5) La CTF controlla che il codice sia nella lista ricevuta dalla CLA. Se c'è, lo segna come usato, per prevenire voti doppi.
- (6) La CTF aggiunge l'ID nella lista delle persone che hanno votato per un candidato e somma 1 al totale.
- (7) Alla fine delle votazioni, la CTF pubblica i risultati insieme alle coppie ID-voto.

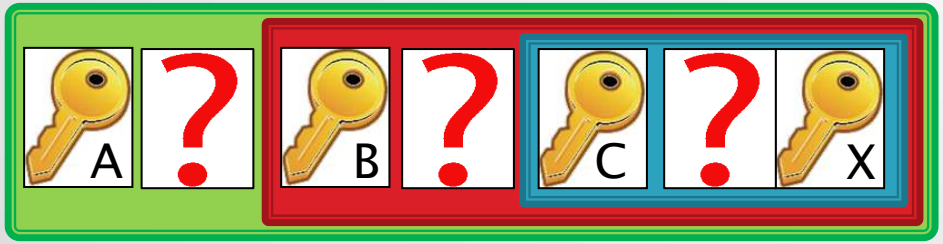
Altri protocolli

- Esistono protocolli con una sola CTF che garantiscono lo stesso livello di sicurezza del precedente, a discapito della semplicità del protocollo.
- Esistono protocolli con nessuna CTF, in cui ogni elettore controlla che gli altri non barino, ma sono così complessi da poter essere implementati solo per gruppi ristretti di persone. Vediamone uno.

Voto senza CTF

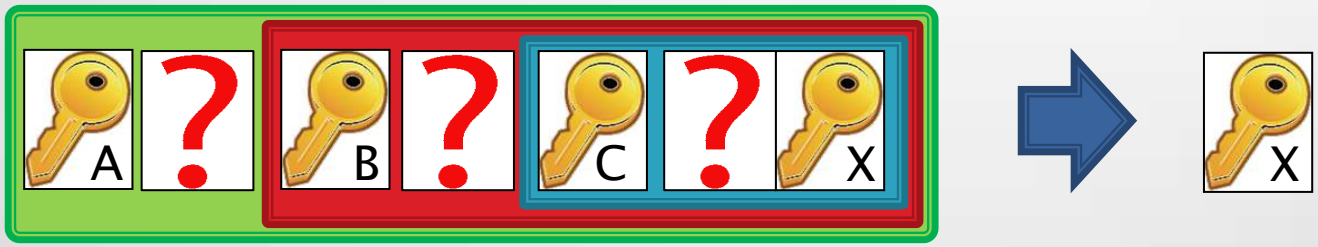
- (0) Alice, Bob e Carol votano si-no (1-0) su un particolare problema. Ognuno ha una chiave privata segreta e una pubblica nota a tutti.
- (1) Ognuno sceglie un voto e fa ciò che segue:



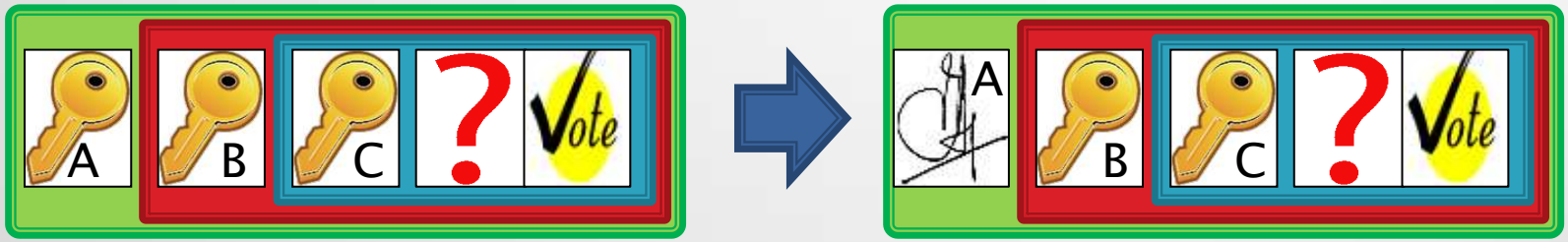


Scrutinio

- (2) Bob e Carol mandano il proprio voto ad Alice, che decritta con la sua chiave privata e toglie tutte le prime stringhe random.
- (3) Alice mescola i voti e li invia a Bob, che ripete il procedimento e invia i voti a Carol.
- (4) Carol ripete il procedimento e li rimanda ad Alice.



- (5) Alice decritta con la sua chiave privata, firma tutti i voti e li rimanda a tutti.
- (6) Bob verifica la firma di Alice e la toglie, ripete il procedimento e li invia a tutti.
- (7) Carol verifica la firma di Bob e la toglie, ripete il procedimento e li invia a tutti.



- **(8)** Ora tutti hanno tre voti firmati da Carol:

- **(9)** Tutti verificano la firma di Carol e la rimuovono. Tutti controllano che ci sia il proprio voto riconoscendo la propria stringa random, e la rimuovono.
- **(10)** Si conteggiano i voti.

Sicurezza del protocollo

- I partecipanti si accorgono immediatamente se qualcuno bara perché ad ogni passo tutti controllano tutti i voti.
- Essendo poche persone, un voto in più si nota subito.
- Sostituire i voti senza essere scoperti è impossibile grazie alle chiavi e alle firme.
- Si può generalizzare a n votanti ma la complessità aumenta.

Secure Multiparty Computation

Simone Coccia

Idea di base

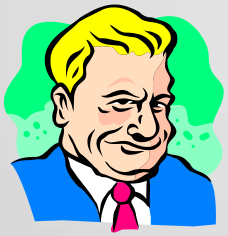
- Protocollo in cui un gruppo di persone possono calcolare insieme qualsiasi funzione di molte variabili in modo particolare
- Ogni partecipante fornisce una o più variabili
- Il risultato della funzione è nota a tutti nonostante nessuno conosca gli input forniti dagli altri membri
- Vedremo vari esempi

Protocollo #1

Come può un gruppo di persone calcolare il loro stipendio medio, senza che nessuno conosca lo stipendio degli altri?

Attori in gioco:

BOB



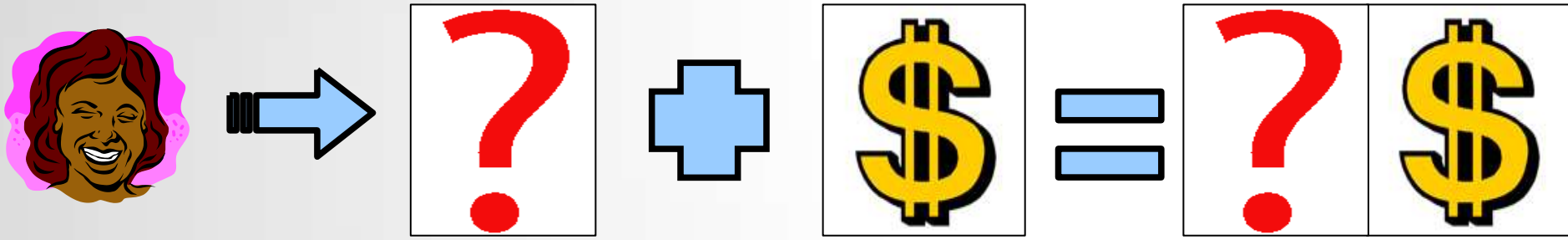
ALICE

CAROL

DAVE

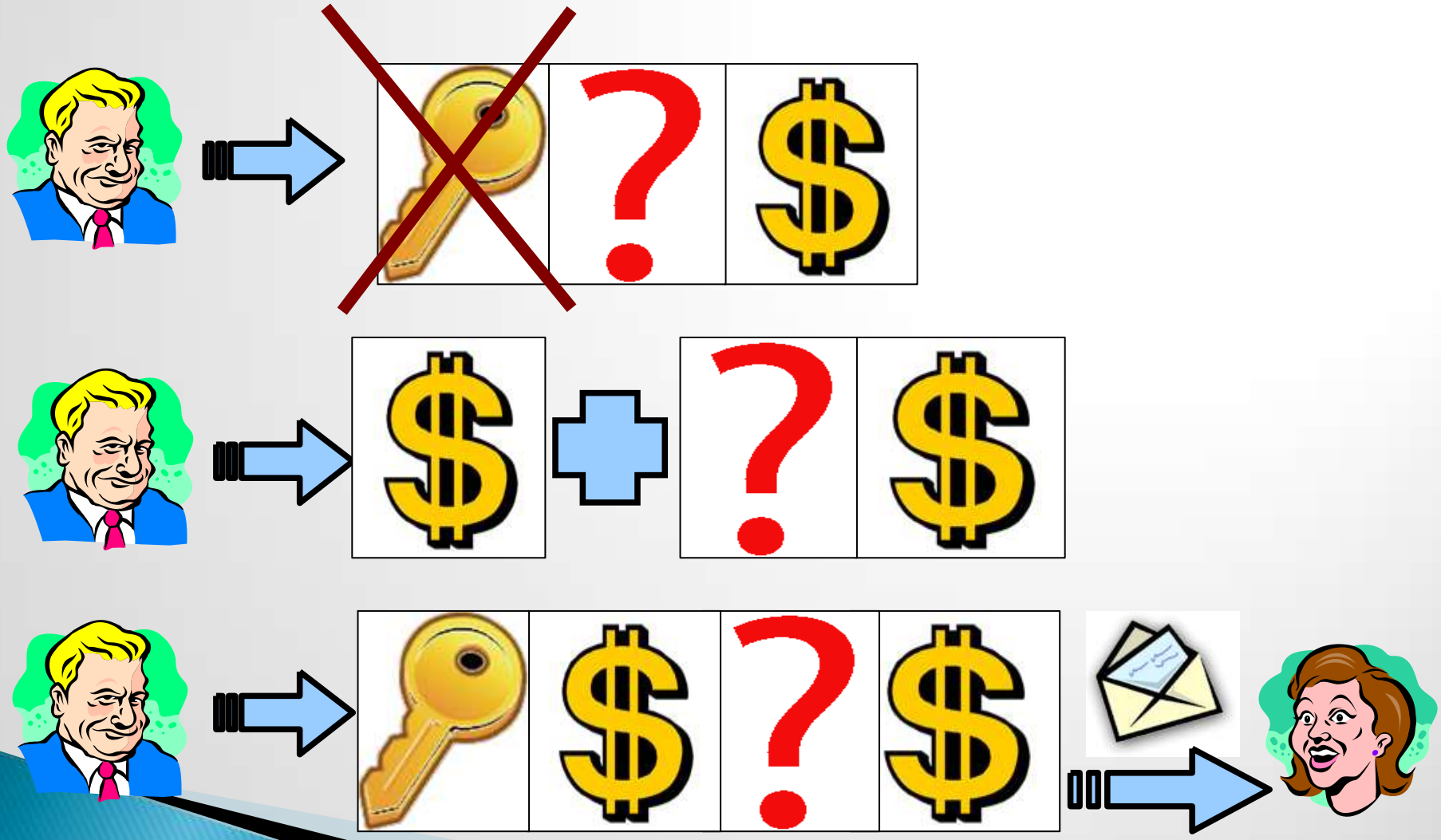
SIMBOLO PER INDICARE LO STIPENDIO

Procedimento – Alice



- Aggiunge un numero segreto a caso al suo stipendio
- Cripta il risultato con la chiave pubblica di Bob
- Invia il risultato a Bob

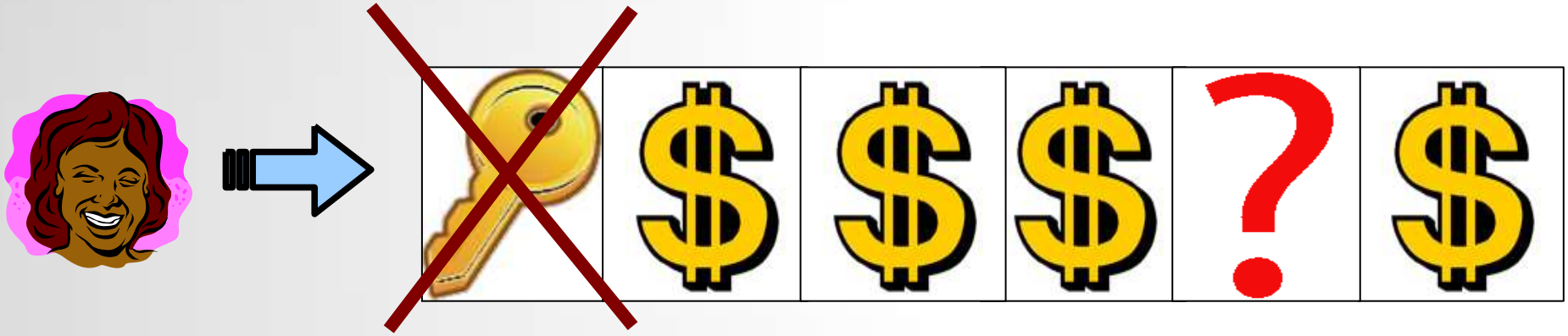
Procedimento – Bob

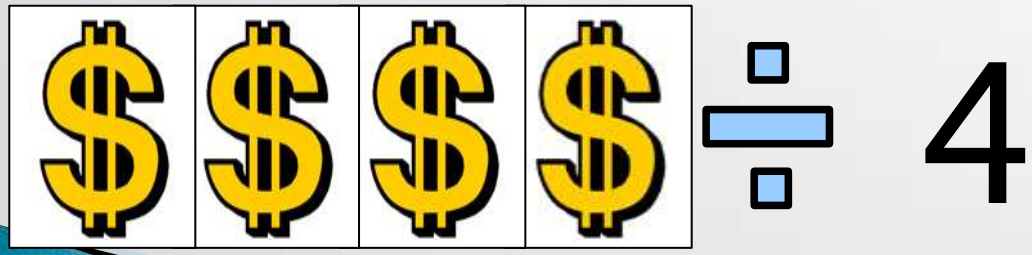


Procedimento – Carol e Dave

- Lo stesso procedimento viene effettuato da Carol e Dave, che rimanda il risultato ad Alice.
- Alice ottiene la somma dei 4 stipendi più il numero random scelto da lei all'inizio.

Procedimento – Nuovamente Alice





4

Ok!
Media
stipendi
trovata!

Caratteristiche e Problematiche

- Implica l'onestà di tutti i partecipanti
- La falsificazione del proprio stipendio comporta una media errata
- Alice potrebbe intuire gli stipendi altrui
- Alice può sottrarre alla fine qualsiasi numero quindi falsare la media

Protocollo #2

Alice e Bob sono a cena insieme in un ristorante e discutono su chi sia più vecchio, ma nessuno vuole dire all'altro la propria età.

Possibile soluzione:

- Entrambi potrebbero dirlo all'orecchio di un cameriere
- Il cameriere confronterebbe a mente i numeri e direbbe chi dei due è il più vecchio

…problematiche

- Il cameriere medio non ha le capacità computazionali per gestire problemi più complessi del confronto di due numeri
- Alice e Bob tengono alla segretezza dei loro dati e potrebbero annegare il cameriere in una pentola di polenta per il timore che lo dica all'amico sommelier.

- Quindi se parla…

Soluzione

La crittografia a chiave pubblica offre una soluzione meno violenta.

Esiste un protocollo per determinare se A<B in cui:

- Alice conosce il valore A
- Bob conosce il valore B
- Alice non riceve ulteriori informazioni su B
- Bob non riceve ulteriori informazioni su A

Problema del milionario di Yao

- Alice conosce l'intero i; Bob conosce l'intero j. Assumiamo che i e j siano nell'intervallo [1,100]. Bob ha una chiave pubblica e una privata.
- (1) Alice sceglie un numero random grande, x, e lo cripta con la chiave pubblica di Bob.

  $c = E_B(x)$
- (2) Alice calcola c – i e invia il risultato a Bob.
- (3) Bob calcola i seguenti 100 numeri:

  $y_u = D_B(c - i + u)$, per ogni u: $1 \leq u \leq 100$
- D_B è la funzione di decriptazione con la chiave privata di Bob.

- **(4)** Bob sceglie un primo random grande, p e calcola i seguenti 100 numeri:

  $z_u = (y_u \bmod p)$, per ogni u: $1 \leq u \leq 100$
- Poi verifica che, per ogni $u \neq v \Rightarrow |z_u - z_v| \geq 2$

  e per ogni $u \Rightarrow 0 < z_u < p - 1$

  Se non sono verificate, Bob sceglie un altro primo p e riprova.
- **(5)** Bob manda ad Alice una sequenza di numeri in quest'ordine:

  $z_1 , z_2 , \ldots, z_j, z_{j+1}+1, z_{j+2}+1, \ldots, z_{100}+1, p$
- **(6)** Alice controlla che l'i-esimo numero nella sequenza è congruente a x mod p. Se si, lei conclude che $i \leq j$. Altrimenti $i > j$.
- **(7)** Alice dice a Bob il risultato del confronto.

Caratteristiche e Problematiche

Questo protocollo non protegge dai ”menzonieri”:

- Alice e Bob possono mentire sulla loro età

Supponendo che i partecipanti non imbroglino volontariamente, è possibile estendere questo protocollo a più partecipanti.

Protocollo #3
(protocollo del Presidente del Consiglio)

- A Silvio piace fare cose strane con gli orsacchiotti di peluche
- Ruby ha fantasie notturne con tavoli di marmo
- Entrambi sono piuttosto imbarazzati dalla loro passione ma gli piacerebbe trovare un compagno adatto
- Esiste un protocollo che gli permette di capire se condividono le stesse fantasie senza svelarle nel caso siano diverse

Come funziona il protocollo

- (1) Si utilizza una funzione one-way: Silvio converte il nome della sua fantasia in una stringa di sette cifre con una funzione hash.
- (2) Silvio utilizza la stringa di sette cifre come un numero di telefono.
- (3) Chiama il numero, e lascia un messaggio per Ruby.
- (4) Se nessuno risponde oppure il numero non è in servizio, Silvio applica una funzione one-way al numero di telefono finché non trova qualcuno che possa sfruttare il protocollo.

Come funziona il protocollo

- (5) Una volta messi in contatto, Silvio dice a Ruby quante volte ha dovuto applicare la funzione alla sua fantasia.
- (6) Ruby applica la funzione hash alla sua fantasia tante volte quanto gli ha detto Silvio.
- (7) Anche lei usa le sette cifre come un numero di telefono e chiede alla persona dell'altra parte se ci sono messaggi per lei.

Chosen-plaintext attack

- Bob ha la possibilità di commettere un attacco chosen-plaintext. Può calcolare la funzione hash di fantasie comuni e chiamare i numeri di telefono risultanti alla ricerca di messaggi per lui.
- Il protocollo funziona solo se ci sono molte fantasie che rendono questo tipo di attacco impraticabile.

Protocollo #4

- Un Consiglio di sette persone si riunisce periodicamente per un scrutinio segreto su determinate questioni (ok lo ammetto! Sono i padroni del mondo)
- Ogni membro del Consiglio può votare sì o no (Yes, No)
- Inoltre due membri hanno la possibilità di dare un super-voto (S-yes, S-no) con diritto di veto.

Processo di voto – esempio 1

Ci sono cinque elettori regolari, N1-N5, e due super-elettori: S1 e S2

La votazione

- Votante: S1 S2 N1 N2 N3 N4 N5
- Voto: S-yes no no no no yes yes

In questo caso l'unico voto che conta è il super-voto S1, la maggioranza di ”no” non conta.

Processo di voto – esempio 2

Ci sono cinque elettori regolari, N1-N5, e due super-elettori: S1 e S2

La votazione

Votante:	S1	S2	N1	N2	N3	N4	N5
Voto:	S-yes	S-no	no	no	no	yes	yes

Qui i due super-voti si annullano e la maggioranza dei regolari "no" decide la questione.

Utilizzo nella realtà

Questo tipo di voto potrebbe verificarsi nella vita reale:

- Per esempio nel consiglio di una società, in cui alcune persone hanno più potere di altri. Oppure
- Nelle procedure di voto delle Nazioni Unite, dove certe nazioni hanno più potere di altre.

Digital Cash

Protocollo per la trasmissione di moneta elettronica

Stefano Limiti

I soldi contanti sono un problema

- Sono scomodi da trasportare
- Sono poco igienici
- E (soprattutto) possono essere rubati

Gli assegni e le carte di credito ne hanno ridotto la quantità fisicamente circolante, ma la sua completa eliminazione è ancora lontana…

Non accadrà mai!

- Sia i trafficanti di droga sia i politici non possono farne a meno…

E la privacy…

D’altra parte, assegni e carte di credito, permettono di invadere a fondo la privacy delle persone:

- Tramite essi è possibile vedere “chi” acquista “cosa” semplicemente da un terminale.

Digital cash

Fortunatamente esiste un complicato protocollo che consente di inviare assegni come messaggi autenticati ma non rintracciabili, nel senso che non possono essere attribuiti a chi li ha compilati.

Caratteristiche:

- Anonimo (privacy venditore-acquirente)
- Non riusabile (assegni non duplicabili)

Digital cash (esempio)

- Silvio può pagare una tangente a Lele trasferendogli del digital cash, senza che Eve venga a sapere l'identità di Silvio.
- Lele può quindi depositare quel denaro elettronico sul proprio conto, anche se la banca non ha idea di chi sia Silvio.
- Se Silvio prova a usare lo stesso digital cash con cui ha corrotto Lele per comprare della cocaina, verrà scoperto dalla banca.

Digital cash (esempio)

- Se Lele prova a depositare lo stesso digital cash in due diversi conti, verrà smascherato, ma in tal caso Silvio rimarrà anonimo.

- Importante! Nei protocolli che vedremo esiste una banca che funge da mediatrice, la cui funzione è generare e convalidare la moneta che Silvio invia a Lele.

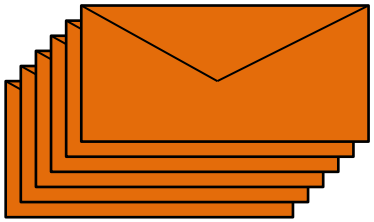
Un primo protocollo

Questo primo protocollo e un protocollo fisico semplificato per assegni anonimi

- (1) Alice prepara 100 assegni anonimi da $1.000 l'uno.
- (2) Alice li mette in cento buste diverse, ognuna contenente un foglio di carta carbone, quindi consegna le buste alla banca.
- (3) La banca apre 99 buste scelte a caso e conferma che tutte contengono un assegno da $1.000.
- (4) La banca firma l'unica busta rimasta sigillata e grazie alla carta carbone tale firma si trasferisce sull'assegno. Quindi la consegna ad Alice e scala $1.000 dal suo conto mettendoli in un conto temporaneo.
- (5) Alice apre la busta e spende l'assegno da un negoziante.
- (6) Il negoziante controlla la firma della banca per assicurarsi che l'assegno sia regolare.
- (7) Il negoziante porta l'assegno in banca.
- (8) La banca verifica la propria firma e versa $1.000 sul conto del negoziante prendendoli dal conto temporaneo.

1) Alice crea gli assegni

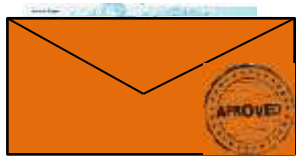
Alice



2) Li invia alla banca

Banca

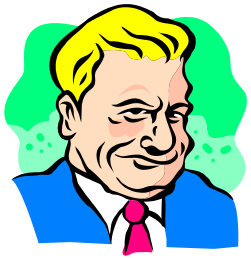
3) La banca apre 99 buste e controlla l'importo degli assegni



5) Lo invia ad Alice

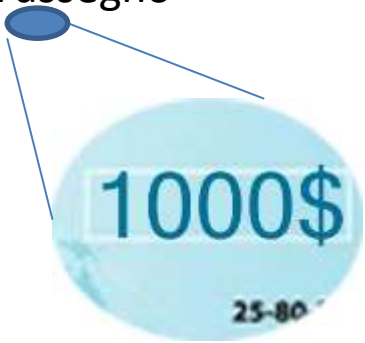
4) Firma l'assegno chiuso

6) Alice usa l'assegno



Bob

8) Bob deposita l'assegno



7) Bob controlla la firma della banca

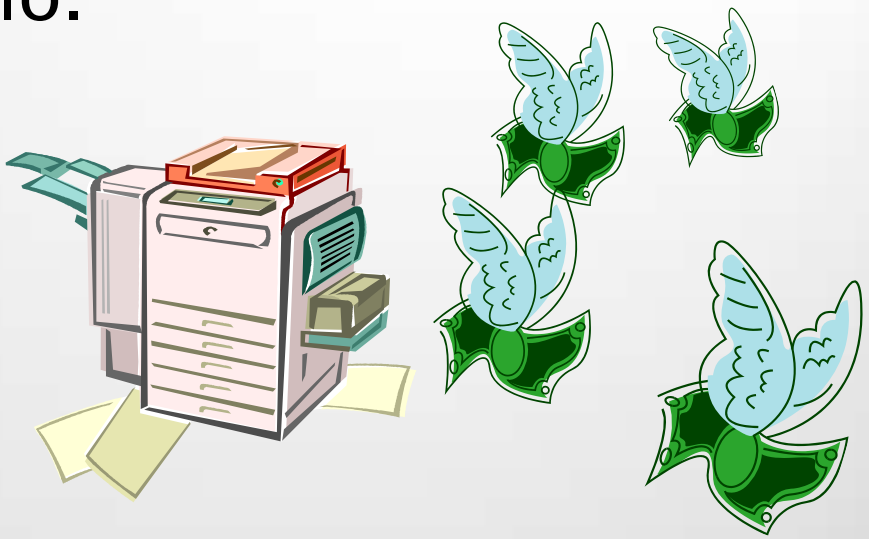
Questo protocollo funziona!

- Viene mantenuto l'anonimato di Alice in quanto la banca firma l'assegno senza vederlo e si tutela sull'effettivo importo dell'assegno grazie alle 99 verifiche che precedono la firma.
- Alice ha solo l' 1% di probabilità di riuscire ad ingannare la banca e se la punizione in caso di truffa è abbastanza severa, non varrà affatto la pena di provare.
- Il protocollo così definito impedisce ad Alice di scrivere un assegno per una cifra più alta di quella dichiarata.

…però…

- Il protocollo non impedisce ad Alice di fotocopiare l'assegno e di spenderlo due volte.

- Per risolvere questo problema bisogna complicare il protocollo.



Protocollo #2

- (1) Alice prepara 100 assegni con l'importo di $1000 ciascuno. Ogni assegno include una stringa casuale significativamente lunga, che lo distingue univocamente
- (2) Alice mette questi 100 assegni, insieme a della carta carbone, in 100 buste sigillate dandole alla banca
- (3) La banca apre 99 di queste buste, scelte a caso fra le 100, e verifica che ci siano assegni da $1000 e che ogni assegno abbia una stringa univoca
- (4) La banca firma l'unica busta rimasta sigillata e grazie alla carta carbone tale firma si trasferisce sull'assegno. A questo punto la banca restituisce ad Alice tale busta detraendo $1000 dal suo conto
- (5) Alice apre la busta e spende l'assegno dal commerciante Bob
- (6) Bob controlla che la firma della banca apposta sull'assegno sia autentica
- (7) Bob incassa l'assegno dalla banca
- (8) La banca verifica nel suo database che un assegno con quella stringa non sia già stato depositato, in tal caso accredita l'importo sul conto di Bob

Pro e Contro

- Grazie alla stringa casuale univoca posta su ogni assegno, la banca si tutela nel caso Alice cercasse di spendere più volte l'assegno e nel caso in cui Bob cercasse di depositarlo più volte
- Ma la banca non riesce a identificare chi è, tra Alice e Bob, un possibile truffatore

Protocollo #3 (1)

- (1) Alice prepara 100 assegni con l'importo di $1000 ciascuno. Ogni assegno include una stringa significativamente lunga, scelta casualmente, che lo distingue univocamente
- (2) Alice mette questi 100 assegni, insieme a della carta carbone, in 100 buste sigillate dandole alla banca
- (3) La banca apre 99 di queste buste, scelte a caso fra le 100, spedite da Alice e verifica che ci siano assegni da $1000 e che ogni assegno abbia una stringa univoca
- (4) La banca firma l'unica busta rimasta sigillata e grazie alla carta carbone tale firma si trasferisce sull'assegno. A questo punto la banca restituisce ad Alice tale busta detraendo $1000 dal suo conto
- (5) Alice apre la busta e spende l'assegno dal commerciante Bob;

Protocollo #3 (2)

- (6) Bob controlla che la firma della banca apposta sull'assegno sia autentica
- (7) Bob chiede ad Alice di scrivere una stringa casuale di identificazione sull'assegno
- (8) Alice accetta
- (9) Bob incassa l'assegno dalla banca
- (10) La banca verifica nel suo database che un assegno con quella stringa non sia già stato depositato, in tal caso accredita l'importo sul conto di Bob e memorizza sia la stringa identificativa dell'assegno che quella di riconoscimento nel database
- (11) Se la stringa di riconoscimento dell'assegno è già presente nel database la banca lo rifiuta. Poi confronta la stringa identificativa sull'assegno con quella memorizzata nel database:
  - se sono uguali allora capisce che Bob è colpevole di aver duplicato l'assegno;
  - altrimenti se sono differenti la banca capisce che Alice ha duplicato l'assegno.

Assunzioni

Il protocollo di Digital Cash così definito è basato su due assunzioni:

- Bob non può modificare la stringa scritta da Alice (danneggiamento dell'assegno)
- Alice deve essere presente nel momento in cui Bob verifica l'assegno con la banca (altrimenti è impossibile risalire a lei nel caso di truffa). Questo è grosso limite.

Verso il protocollo definitivo…

Definiamo una variante del protocollo grazie al quale la banca può scoprire l'identità di Alice nel momento in cui tenta di imbrogliare, riuscendo a fare ciò che il protocollo precedente non poteva.

- Per fare ciò è necessario utilizzare il protocollo di Secret Splitting (visto a lezione)

Primo passo

- (1) Alice prepara 100 assegni anonimi da $1000 ciascuno. Ognuno di essi contiene:
  - Ammontare: $1000;
  - Stringa di riconoscimento assegno: X;
  - Stringhe di identità:
    - $I_1 (I_{1L}, I_{1R}), I_2 (I_{2L}, I_{2R}) \ldots I_{100} (I_{100L}, I_{100R})$.

Stringhe identità

Ogni coppia è generata in questo modo:

- Alice crea una stringa contenente il proprio nome, il proprio indirizzo ed ogni altra informazione richiesta dalla banca.

- Quindi la divide in due frammenti, usando il protocollo di secret splitting;

- Per es.: I_{37} è composto da due stringhe I_{37L} e I_{37R} che, a richiesta della banca, possono essere aperte da Alice in ogni momento

- Ogni coppia rivela l'identità di Alice.

- Quindi ogni assegno è composto da:
  - un importo
  - una stringa di riconoscimento per l'assegno
  - delle stringhe di identità

- (2) Alice nasconde i 100 assegni con il protocollo blind signature (visto in precedenza) e spedisce tutto alla banca
- (3) La banca apre 99 di queste buste, scelte a caso fra le 100, e verifica che siano assegni da $1000, verifica la stringa di riconoscimento e chiede ad Alice di rivelare le stringhe di identità.

- (4) Nel caso in cui tali controlli siano andati a buon fine la banca firma l'assegno non scoperto ad Alice e detrae $1000 dal suo conto
- (5) Alice apre la busta e spende l'assegno da un commerciante Bob
- (6) Bob controlla che la firma della banca apposta sull'assegno sia autentica
- (7) Bob consegna ad Alice una stringa di 100 bit scelta a caso, $b_1\, b_2 \ldots b_{100}$ e chiede di aprire la parte destra o sinistra di ciascuna delle stringhe di identità poste sull'assegno; Alice aprirà la parte sinistra o destra di I_i a seconda se b_i sia 0 oppure 1

- (8) Bob incassa l'assegno dalla banca;
- (9) La banca verifica nel suo database che un assegno con quella stringa non sia già stato depositato, in tal caso accredita l'importo sul conto di Bob e memorizza la stringa identificativa dell'assegno, quella di riconoscimento e le altre informazioni identificative nel database

- (10) Se la stringa di riconoscimento dell'assegno è già presente nel database la banca lo rifiuta. Poi confronta la stringa identificativa sull'assegno con quella memorizzata nel database:
  - se sono uguali allora capisce che Bob è colpevole di aver duplicato l'assegno;
  - altrimenti se sono differenti la banca capisce che Alice ha duplicato l'assegno
  - siccome Alice ha riutilizzato l'assegno con un altro commerciante Carl, quest'ultimo avrà dato ad Alice una stringa casuale di 100 bit differenti da quella datagli da Bob. La banca ricerca una coppia che, combinando i risultati delle due differenti aperture, abbia entrambe le metà svelate.

Considerazioni

- Con questo protocollo Alice può provare a spendere due volte lo stesso assegno e ci riuscirà solo se le stringhe di selezione ($b_1\ b_2 \ldots b_{100}$) sono identiche. La probabilità che le due stringhe di 100 bit siano uguali è $1/2^{100}$ quindi trascurabile.

- Alice può anche provare a far firmare alla banca un assegno con le stringhe d'identità sbagliate, magari con l'identità di qualcun altro, in questo caso le probabilità sono una su n (=100), quindi decisamente migliori. Per ovviare a questo problema il libro suggerisce la galera.

Considerazioni

- Il negoziante (Bob) non può fare praticamente nulla per imbrogliare.
- La banca, naturalmente, non può conoscere l'identita di Alice (se non truffa), nemmeno con l'aiuto del negoziante.
- L'unica che può imbrogliare è Eve. Se ascolta la comunicazione tra Alice e il negoziante e riesce ad arrivare in banca prima di quest'ultimo, può incassare l'assegno.

Il Crimine Perfetto

Come abbiamo visto sino ad ora l'anonimato risulta essere fondamentale per le transazioni con moneta elettronica. Ma lo stesso anonimato può essere usato per scopi illeciti come mostra il seguente protocollo.

Il Crimine Perfetto

- Bob rapisce un bambino
- Bob prepara 10.000 assegni anonimi di qualsiasi cifra
- Bob nasconde questi assegni con il protocollo blind signature e manda tutto alle autorità con le seguenti richieste che se non esaudite comporterebbero l'uccisione del bambino:
  - una banca deve firmare tutti gli assegni
  - la banca deve pubblicare i risultati su di un giornale
  - le autorità devono accettare
- Bob verifica l'avvenuta pubblicazione, scopre gli assegni e li spende (alle Maldive)
- Ah, e per ultimo Bob rilascia il bambino! (non alle Maldive!)

Grazie dell'attenzione!

Note di produzione:
Nessun orsetto di peluche è stato maltrattato durante la stesura di queste slide.