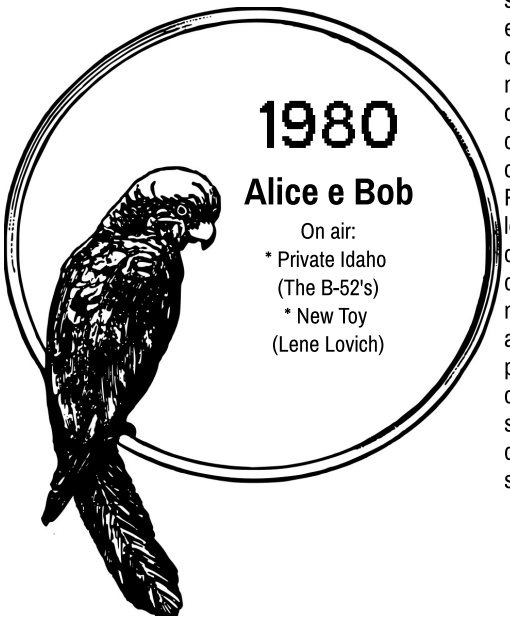
Hack (or) Wave

una radiofanzine su storia dei computer e musica new wave

Alice e Bob sono i nomi di due personaggi utilizzati nella maggior parte dei testi di crittografia, diventati popolari attraverso l'invenzione e popolarizzazione di un algoritmo avvenuta tra la fine degli anni '70 e l'inizio degli anni '80: usiamo quindi il 1980 come anno di mezzo per raccontare qualcosa sulla crittografia attraverso la storia di Alice e Bob.

La crittografia è una scienza abbastanza vecchia, legata alla matematica, al linguaggio e alla scrittura di algoritmi. Negli anni '70 c'è una grande svolta grazie all'invenzione della crittografia a chiave pubblica, che semplificó enormemente le operazioni necessarie per cifrare le comunicazioni tra computer. Precedentemente lo scambio della chiave tramite cui decifrare i messaggi doveva avvenire di persona o comunque secondo procedure di sicurezza molto stringenti.



Nel 1977 un team di tre scienziati, Ronald Rivest, Adi Shamir e Leonard Adleman, iniziano a lavorare a questa funzione necessaria per generare le chiavi. La storia qui prende una fondamentale svolta alcolica: i tre raccontano che Rivest ebbe l'illuminazione necessaria per concludere il lavoro dopo aver bevuto troppo vino durante una cena in occasione della pasqua ebraica. Poco dopo i tre pubblicano un report in cui spiegano la loro soluzione, che effettivamente funzionava: questa soluzione diventerá il famoso algoritmo RSA, dalle loro iniziali.

Algoritmo RSA

Key Generation

Select two prime number, p, and q.
Calculate n = pxq
Calculate $\phi(n) = (p-1)x(q-1)$
Select integer a, $gcd(\phi(n), a) = 1; 1 < a < \phi(n)$
Calculate b
Public Key: KU = {a, n}
Private Key: KR = {b, n}

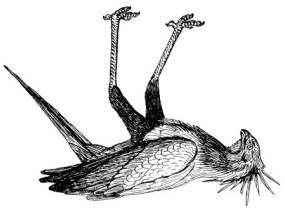
Encryption

Plaintext: $M < n$
Ciphertext: $C = M^a \pmod n$

Decryption

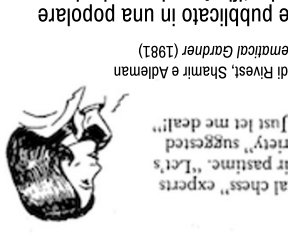
Ciphertext: C
Plaintext: $M = C^d \pmod n$

"I want a New Toy (oh ay oh), to keep my head expanding (ta)
I want a New Toy (oh ay oh), nothing too demanding (ta)
Then when everything is in roses everything is static (ta)
Yeh my New Toy (oh ay oh), you'll find us in the attic"
Lene Lovich, New Toy (1981)



Bob si stabiliscono come "la coppia più famosa della crittografia". Nel 1981 un articolo di Manuel Blum inizia ad aggiungere dettagli alla storia di Alice e Bob: stanno divorziando e devono decidere chi tiene la macchina. Un'altra storiella famosa viene raccontata nel 1984 dal crittografo John Gordon. Gordon usa Alice e Bob per spiegare l'applicazione della crittografia al mercato azionario: Bob è un broker, mentre Alice una speculatrice sul mercato azionario e stanno facendo truffe alle assicurazioni. Gli sbirri americani li cercano e in più Alice vuole nascondere a suo marito la vera natura della sua professione.

Nello stesso anno l'algoritmo viene pubblicato in una popolare rubrica di giochi matematici su Scientific American, che lo renderá famoso. Al tempo stesso però attira anche le attenzioni dell'intelligence americana, in quanto ai tempi la crittografia era considerata da un punto di vista giuridico come una "munizione" nel senso militare del termine, dunque la sua circolazione era tenuta sotto controllo e non era così liberamente fruibile. I nostri comunque vanno avanti. Nel 1978 rpubblicano l'articolo su una rivista scientifica, ed è qui che appaiono per la prima volta Alice e Bob: sono usati come esempi del modo in cui le entità coinvolte nella comunicazione da cifrare si organizzano. Prima si usava solo "A" e "B", ma per Rivest, Shamir e Adleman è più comodo usare i nomi. Dopo questa prima menzione, Alice



Once there were two "mental chess" experts who had become tired of their pastime. "Let's play 'Mental Poker,' for variety" suggested one. "Sure" said the other. "Just let me deal!"

Alice e Bob in "Mental Poker", articolo di Rivest, Shamir e Adleman pubblicato nella raccolta *The Mathematical Gardner* (1981)

Bibliografia:

* Diffie, W.; Hellman, M.E. (1976). "New directions in cryptography". IEEE Transactions on Information Theory. 22 (6): 644–654
* Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21(2), 120-126.
* Parthasarathy, S. (2013). Alice and Bob can go on a holiday!. Algologic Technical Report 11/2012.
* http://cryptocouple.com/

Da en.wikipedia.org:
* Alice and Bob
* RSA (cryptosystem)
* Public-key cryptography

Questa zine è stata prodotta a marzo 2019 da Hack or Wave

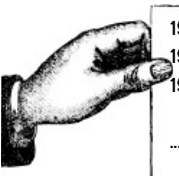
Testi ed elaborazione grafica sono rilasciati sotto una licenza
CC-BY-NC-SA 4.0 Internazionale

Testo: https://creativecommons.org/licenses/by-nc-sa/4.0/legalcode.it

Se non specificato altrimenti le immagini sono in pubblico dominio o prese in prestito per motivi di studio e ricerca.

fine

Hack or Wave, nelle puntate precedenti:



1977: il Personal Computer
1978: informatica in India
1979: Usenet

...fino al 1989 (forse)

collezionaci tutte!

Da oggi con guide per rilegatura DIY incluse! Fai un buco in corrispondenza dei cerchi a lato pagina e poi assicura le tue preziosissime fanzine con un cordino, un laccio, un nastro o il filo delle cuffie.

o ascoltaci!

https://hackordie.gattini.ninja

Note:

1980: Alice e Bob

Questa procedura divenne sempre piú inefficiente con l'espandersi dei network tra computer, in quanto all'apertura di un nuovo nodo era necessario procedere ogni volta con un passaggio fisico delle chiavi. C'era bisogno di una chiave che potesse essere scambiata senza troppe paranoie sulla sicurezza, cioé una chiave che in qualche modo potesse essere pubblica.

Dei primi esperimenti su come provare a risolvere questo problema vengono fatti giá all'inizio negli anni '70 dall'intelligence britannica. Ma all'inizio questi progetti sono tenuti confidenziali e solo anni dopo furono resi pubblici, quando giá altri ricercatori avevano pubblicato sull'argomento.

Ma non importa se sei Alice o Bob o Sita o Rama o leone o gazzella: proteggi le tue comunicazioni e la tua privacy con la crittografia tutte le volte che puoi!

Disegna qui le tue Alice e Bob e i loro nemici

Nome:_ _ _ _ _ _ _ _
(SENDER)

Nome:_ _ _ _ _ _ _ _
(ATTACKER)

Nome:_ _ _ _ _ _ _ _
(RECEIVER)

Schema di funzionamento della crittografia a chiave pubblica

La crittografia a chiave pubblica viene per la prima volta presentata alla comunitá accademica nel 1976, quando i ricercatori Whitfield Diffie e Martin Hellman mettono appunto una teoria per un sistema crittografico basato su due parti: una pubblica e una privata. Tramite questo sistema si eliminava il passaggio fisico della consegna della chiave perché consentiva di condividerne una parte in luoghi "pubblici" e al tempo stesso averne una parte privata da tenere al sicuro e usare per leggere i messaggi. Diffie ed Hellman pubblicano un articolo in cui spiegano questo loro modello, che genera molto interesse. Tuttavia, manca ancora una funzione che permetta effettivamente di generare queste due chiavi, in quanto il modello presentato era solo teorico.

"Keep off the path, beware of the gate, watch out for signs that say "hidden driveways". Don't let the chlorine in your eyes blind you to the awful surprise that's waitin' for you at the bottom of the bottomless blue blue pool."

The B-52s, Private Idaho (1980)

Nel corso del tempo, la coppia Alice e Bob diventerá l'esempio per eccellenza nei testi di crittografia, ma non solo: la criptocoppia si diffonderá anche in altre discipline come l'economia, la fisica e l'ingegneria. Dal 1985 arrivano anche altri personaggi. La prima è Eve la spiona (dall'inglese "eavesdropper"), che è un terzo elemento che si inserisce nella conversazione per ascoltarla. Negli anni successivi ci saranno anche altri personaggi: Craig il Password Cracker, che vi cracca le password; Grace la rappresentante del governo, che costringe Alice e Bob a implementare una backdoor nei loro protocolli; Mallory il Malicious Attacker e Oscar l'Opponente, che non è necessariamente malvagio; Trudy l'intrusa, che sarebbe stata bene anche tra gli Sgorbions; il guardiano Walter e Wendy la Wistleblower, cioè la Snowden della situazione che ha un accesso privilegiato alle informazioni e le divulga all'esterno della cerchia privata. Alice e Bob sono carini, ma hanno anche subito critiche. Per esempio Parthasarathy, crittografo indiano, ha deciso di utilizzare Sita e Rama (sender e receiver) invece di Alice e Bob come forma di decolonizzazione della crittografia. Abbiamo anche critiche femministe, scaturite soprattutto dall'arrivo di Eve, la quale ha generato una situazione in cui Alice ed Eve sono nulla piú che gli stereotipi di donna-mogile e donna-amante che vivono in funzione di Bob.

Sì ringraziano: