

Crittografia a chiave pubblica: uno sguardo alle vulnerabilità di RSA e Diffie-Hellman



Leonardo Alfредucci

Relatori

Dott. Gaspare Ferraro

Prof.ssa Anna Bernasconi

Università di Pisa

Dipartimento di Informatica

Pisa, 7 ottobre 2022

Indice

① Introduzione

② RSA



Parte 1

Introduzione



Introduzione

- Una grandissima quantità di informazioni viaggia attraverso la rete: è dunque di fondamentale importanza proteggere i dati che vengono scambiati.
- Si passeranno in rassegna i due protocolli più usati per lo scambio di chiave: RSA e Diffie-Hellman, quest'ultimo analizzato su campo primo e su curve ellittiche.
- Lo scopo della tesi è quello di andare al di là di una trattazione teorica di questi due protocolli, concentrandosi piuttosto sull'aspetto pratico.



Parte 2

RSA



La teoria di RSA

- È un cifrario asimmetrico. Sono dunque presenti due coppie di chiavi:
 - (e, n) utilizzata per cifrare (*chiave pubblica*);
 - (d, n) utilizzata per decifrare (*chiave privata*).
- Si scelgono due numeri primi p e q .
- Si calcola $n = p \cdot q$ e $\phi(n) = (p - 1) \cdot (q - 1)$.
- Si sceglie $e < \phi(n)$ tale che $\gcd(e, n) = 1$.
- Si calcola $d = e^{-1} \bmod \phi(n)$.
- Tutti i passi descritti possono essere svolti in tempo polinomiale.



RSA: cifratura e decifrazione

- Per cifrare un messaggio m è sufficiente calcolare il crittogramma c come:

$$c = m^e \mod n.$$

- Per ottenere il messaggio m dato c è sufficiente calcolarlo come:

$$m = c^d \mod n.$$



La sicurezza di RSA 1

- La sicurezza di RSA è garantita grazie al problema della fattorizzazione di un numero n come prodotto di due fattori $p \cdot q$.
- Per questo è importante scegliere due fattori primi molto grandi, tale che il modulo sia almeno 2048 bit, meglio ancora se 3072 bit.
- Nel 1999 è stato fattorizzato RSA-512 in circa 7 mesi utilizzando centinaia di calcolatori e impiegando l'equivalente di 8400 anni di CPU.
 - Nel 2009 lo stesso attacco poteva essere effettuato in 83 giorni da un solo calcolatore.
- Nel 2020 il numero più grande fattorizzato ha 829 bit, impiegando l'equivalente di 2700 anni di CPU.



La sicurezza di RSA 2

- Sono stati implementati tre algoritmi per la fattorizzazione:
 - *Wheel factorization*: fondamentalmente un brute force sul numero, cercando i divisori;
 - *Pollard's rho factorization*: di natura probabilistica, è quello più efficiente;
 - *Fermat factorization*: è più veloce se i due numeri primi sono vicini tra loro.
- Sono stati fattorizzati moduli da 120 bit utilizzando l'algoritmo *Pollard's rho* in poco meno di un'ora su un moderno calcolatore.



RSA: Valori più utilizzati di e

<i>X.509</i>			<i>PGP</i>			<i>Combinati</i>		
e	$hm(e)$	%	e	$hm(e)$	%	e	$hm(e)$	%
65537	2	98.4921	65537	2	48.8501	65537	2	95.4933
17	2	0.7633	17	2	39.5027	17	2	3.1035
3	2	0.3772	41	3	7.5727	41	3	0.4574
35	3	0.1410	19	3	2.4774	3	2	0.3578
5	2	0.1176	257	2	0.3872	19	3	0.1506
7	3	0.0631	23	4	0.2212	35	3	0.1339
11	3	0.0220	11	3	0.1755	5	2	0.1111
47	5	0.0101	3	2	0.0565	7	3	0.0596
13	3	0.0042	21	3	0.0512	11	3	0.0313
65535	16	0.0011	$2^{127} + 3$	3	0.0248	257	2	0.0241
altri	-	0.0083	altri	-	0.6807	altri	-	0.0774



