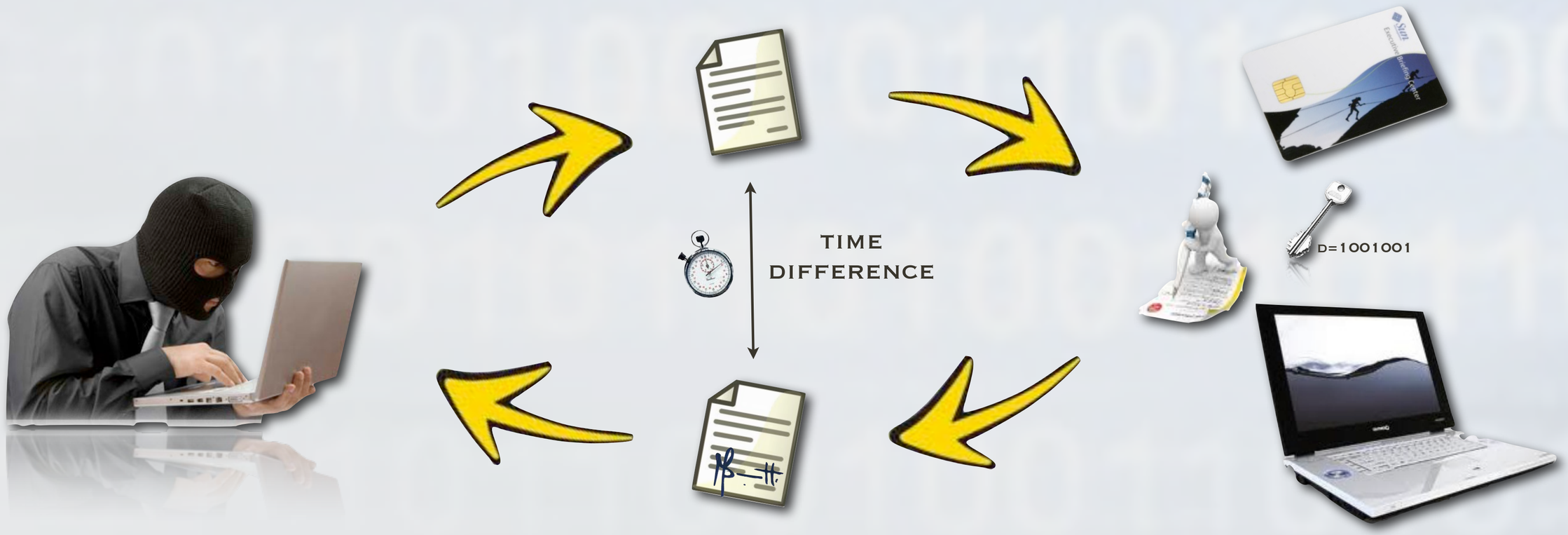
TIMING ATTACK AD RSA

MARCO CALDERINI

IDEA DEL TIMING ATTACK

- GLI ALGORITMI DI CRITTOGRAFIA ESEGUONO I CALCOLI IN TEMPI NON COSTANTI



- L'IDEA DI BASE È SFRUTTARE QUESTE MISURAZIONI PER OTTENERE INFORMAZIONI SULLA CHIAVE PRIVATA

RSA

- crittosistema a chiave pubblica ideato da Rivest, Shamir e Adleman nel 1978

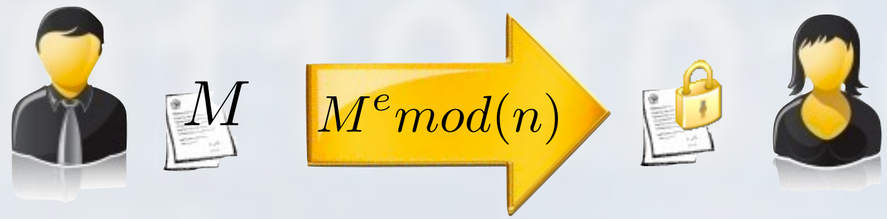
- generare le chiavi pubbliche e le chiavi private

  - ✓ si generano due numeri primi p e q distinti
  - ✓ si calcolano $n = pq$ e $\phi(n) = (p-1)(q-1)$
  - ✓ si sceglie $e \in \mathbb{Z}_{\phi(n)}$ tale che $MCD(e, \phi(n)) = 1$
  - ✓ si calcola $d \in \mathbb{Z}_{\phi(n)}$ tale che $de \equiv 1 mod(\phi(n))$
  - ✓ la chiave pubblica sarà (e, n) e quella privata (d, n)

RSA

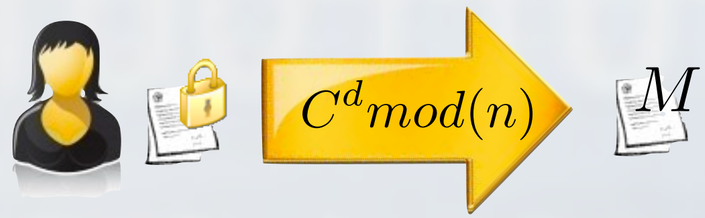
CIFRATURA

$$C = M^e mod(n)$$



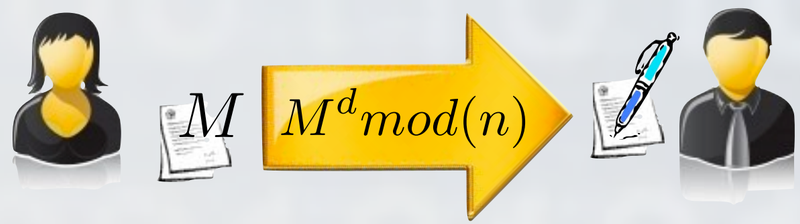
DECIFRATURA

$$M = C^d mod(n) = M^{ed} mod(n)$$



FIRMA

$$S = M^d mod(n)$$



ALGORITMO LEFT-TO-RIGHT

- ALGORITMO PROPOSTO DA RIVEST, SHAMIR E ADLEMAN PER SVOLGERE L'ESPONENZIALE MODULARE

IMPUT: $M, N, d = (d_{w-1}...d_0)_2$
OUTPUT: $S = M^d mod(N)$

1. $S \leftarrow 1$;
2. **for** $j = w - 1$ **to** 0 **do**
3. $S \leftarrow S^2 mod(N)$;
4. **if** $d_j == 1$ **then**
5. $S \leftarrow SM mod(N)$;
6. **return** S.

SE IL BIT È 0 VIENE CALCOLATO SOLO IL QUADRATO

SE IL BIT È 1 VIENE CALCOLATO IL QUADRATO E LA MOLTIPLICAZIONE

TIMING ATTACK

- L'attaccante chiede ad Alice di firmare i messaggi $M_1, ..., M_k$ e memorizza i tempi necessari alle firme $T_1, ..., T_k$

- L'attaccante ha a disposizione un PC identico a quello di Alice così da poter riprodurre i calcoli dell'algoritmo left-to-right con gli stessi tempi

- L'attaccante inizia a calcolare i cicli iterativi del FOR, uno alla volta ipotizzando ogni volta il valore del bit dell'esponente

TIMING ATTACK

- Per cominciare si considera il bit d_{w-1}

ipotesi $d_{w-1} = 0 \Longrightarrow$ firmo $\widetilde{M}_i$ con l'esponente 0 e ottengo il tempo $\widetilde{T}_{i,w-1,0}$

ipotesi $d_{w-1} = 1 \Longrightarrow$ firmo $\widetilde{M}_i$ con l'esponente 1 e ottengo il tempo $\widetilde{T}_{i,w-1,1}$

0	1
$T_1 - \widetilde{T}_{1,w-1,0}$	$T_1 - \widetilde{T}_{1,w-1,1}$
$\vdots$	$\vdots$
$T_k - \widetilde{T}_{k,w-1,0}$	$T_k - \widetilde{T}_{k,w-1,1}$

- calcolo $S_0^2 = \dfrac{1}{k-1}\sum_{i=1}^{k}(T_{i,0} - \overline{T}_0)^2$ $\qquad$ $S_1^2 = \dfrac{1}{k-1}\sum_{i=1}^{k}(T_{i,1} - \overline{T}_1)^2$

$T_i - \widetilde{T}_{i,w-1,0}$ — MEDIA DIFFERENZE

- scelgo il bit che da la varianza minore

TIMING ATTACK

- SIA ORA d_b UN BIT GENERICO E $d_{w-1}, ..., d_{b+1}$ CALCOLATI CORRETTAMENTE

IPOTESI $d_b = 0 \Longrightarrow$ FIRMO M_i CON L'ESPONENTE $d_{w-1}...d_{b+1}0$ E OTTENGO IL TEMPO $\widetilde{T}_{i,b,0}$

IPOTESI $d_b = 1 \Longrightarrow$ FIRMO M_i CON L'ESPONENTE $d_{w-1}...d_{b+1}1$ E OTTENGO IL TEMPO $\widetilde{T}_{i,b,1}$

- CALCOLO S_0^2 E S_1^2

- SCELGO IL BIT CHE DA LA VARIANZA MINORE

TIMING ATTACK IN DETTAGLIO

Il tempo necessario per firmare un messaggio M_i è

$$T_i = e_i + \sum_{j=0}^{w-1} (s_{i,j} + t_{i,j})$$

- e_i: errori di misurazione
- $s_{i,j}$: tempo di calcolo del quadrato
- $t_{i,j}$: tempo di calcolo del prodotto

Il tempo necessario per firmare un messaggio M_i con l'esponente $d_{w-1}...d_{b+1}h$ dove h è l'ipotesi per il bit d_b è

$$\widetilde{T}_{i,b,h} = \sum_{j>b} (s_{i,j} + t_{i,j}) + (s_{i,b} + \widetilde{t}_{i,b,h})$$

$\widetilde{t}_{i,b,h}$: candidato per $t_{i,b}$

TIMING ATTACK IN DETTAGLIO

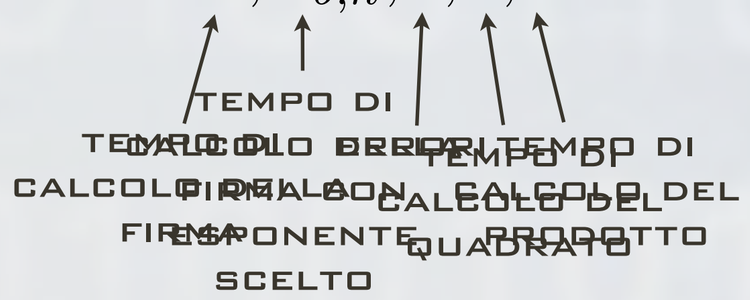
- SE L'IPOTESI SU d_b È CORRETTA

$$T_i - \widetilde{T}_{i,b,h} = e_i + \sum_{j<b}(s_{i,j} + t_{i,j})$$

- SE L'IPOTESI SU d_b È ERRATA

$$T_i - \widetilde{T}_{i,b,h} = e_i + \sum_{j<b}(s_{i,j} + t_{i,j}) + (t_{i,b} - \widetilde{t}_{i,b,h})$$

CONSIDERIAMO LE VARIABILI ALEATORIE $T, \widetilde{T}_{b,h}, e, s, t$



TIMING ATTACK IN DETTAGLIO

- VARIANZA IPOTESI CORRETTA

$$Var(T - \widetilde{T}_{b,h}) = Var\left(e + \sum_{j<b} s + \sum_{\substack{j<b \\ d_j \neq 0}} t\right)$$

$$= Var(e) + bVar(s) + lVar(t)$$

NUMERO BIT NON NULLI

- VARIANZA IPOTESI ERRATA

$$Var(T - \widetilde{T}_{b,h}) = Var(e) + bVar(s) + (l+1)Var(t)$$

CON L'IPOTESI ERRATA ABBIAMO UNA VARIANZA MAGGIORE DI $Var(t)$

PROBABILITÀ DI SUCCESSO

- $s - \mathcal{N}(\mu_s, \sigma_s^2)$ E $t - \mathcal{N}(\mu_t, \sigma_t^2)$

- $\sum_{j<b} s + \sum_{\substack{j<b \\ d_j \neq 0}} t - \mathcal{N}(\mu_0, \sigma_0^2)$ E $\sum_{j<b} s + \sum_{\substack{j<b \\ d_j \neq 0}} t + t - \mathcal{N}(\mu_0 + \mu_t, \sigma_0^2 + \sigma_t^2)$

VARIABILE ALEATORIA RELATIVA COLONNA CORRETTA

VARIABILE ALEATORIA RELATIVA COLONNA ERRATA

DOVE $\mu_0 = b\mu_s + l\mu_t$ E $\sigma_0^2 = b\sigma_s^2 + l\sigma_t^2$

PROBABILITÀ DI SUCCESSO

Consideriamo ora le k misurazioni del tempo delle firme e indichiamo con X e Y le variabili normali standardardizzate corrette ed errate rispettivamente, possiamo scrivere la tabella $(Var(e) \approx 0)$

$\sigma_0 X_1 + \mu_0$	$(\sigma_0 X_1 + \mu_0) + (\sigma_t Y_1 + \mu_t)$
$\vdots$	$\vdots$
$\sigma_0 X_k + \mu_0$	$(\sigma_0 X_k + \mu_0) + (\sigma_t Y_k + \mu_t)$

COLONNA CORRETTA

COLONNA ERRATA

PROBABILITÀ DI SUCCESSO

- PONIAMO $V_i = \sigma_0 X_i + \mu_0$ E $W_i = (\sigma_0 X_i + \mu_0) + (\sigma_t Y_i + \mu_t)$

$$Pr(S_W^2 > S_V^2) = Pr\left(\frac{1}{k-1}\sum_{i=1}^{k}(W_i - \overline{W})^2 > \frac{1}{k-1}\sum_{i=1}^{k}(V_i - \overline{V})^2\right)$$

$$= Pr\left(\sum_{i=1}^{k}(W_i - \overline{W})^2 > \sum_{i=1}^{k}(V_i - \overline{V})^2\right).$$

PROBABILITÀ DI SUCCESSO

- SE k È SUFFICIENTEMENTE GRANDE

$$\overline{V} \approx \mu_0 \qquad \overline{W} \approx \mu_0 + \mu_t$$

$$\Downarrow$$

$$Pr(S_W^2 > S_V^2) \approx Pr\left(\sum_{i=1}^{k}(\sigma_0 X_i + \sigma_t Y_i)^2 > \sum_{i=1}^{k}(\sigma_0 X_i)^2\right)$$

$$= Pr\left(\sum_{i=1}^{k}(\sigma_0^2 X_i^2 + \sigma_t^2 Y_i^2 + 2\sigma_0\sigma_t X_i Y_i) > \sum_{i=1}^{k}(\sigma_0^2 X_i^2)\right)$$

$$= Pr\left(\sum_{i=1}^{k}(2\sigma_0\sigma_t X_i Y_i) + \sum_{i=1}^{k}(\sigma_t^2 Y_i^2) > 0\right)$$

$$= Pr\left(2\sigma_0 \sum_{i=1}^{k} X_i Y_i + \sigma_t \sum_{i=1}^{k} Y_i^2 > 0\right)$$

PROBABILITÀ DI SUCCESSO

- X E Y SONO INDIPENDENTI $\Longrightarrow E(XY) = E(X)E(Y) = 0$
- X E Y SONO STANDARDIZZATE $\Longrightarrow E(X^2) = E(Y^2) = 1$

$$\sum_{i=1}^{k} Y_i^2 \approx \sum_{i=1}^{k} E\left(Y^2\right) = k$$

$$\begin{aligned} Var(XY) &= E(X^2Y^2) - E(XY)^2 \\ &= E(X^2Y^2) = E(X^2)E(Y^2) = 1 \end{aligned}$$

- PER IL TEOREMA DEL LIMITE CENTRALE $\sum_{i=1}^{k} X_i Y_i$ SEGUE LA DISTRIBUZIONE $\mathcal{N}(0, k)$
- $\sum_{i=1}^{k} Y_i^2$ SI PUÒ APPROSSIMARE CON k

PROBABILITÀ DI SUCCESSO

- SIA Z UNA VARIABILE CASUALE STANDARDIZZATA

$$Pr(S_W^2 > S_V^2) \approx Pr(2\sigma_0(\sqrt{k}Z) + \sigma_t k > 0) = Pr\left(Z > -\frac{\sigma_t}{\sigma_0}\frac{\sqrt{k}}{2}\right) = \Phi\left(\frac{\sigma_t}{\sigma_0}\frac{\sqrt{k}}{2}\right)$$

AREA SOTTESA DALLA CURVA NORMALE STANDARD

- $\sigma_0^2 = b\sigma_s^2 + l\sigma_t^2$, SUPPONIAMO INOLTRE $l = \frac{3}{4}b$

$$Pr(S_W^2 > S_V^2) \approx \Phi\left(\frac{\sqrt{k}}{\sqrt{b\left(4\frac{\sigma_s}{\sigma_t} + 3\right)}}\right)$$

COL DECREMENTARE DI b E AUMENTANDO IL NUMERO DI MESSAGGI k, AUMENTA LA PROBABILITÀ DI DETERMINARE LA CHIAVE PRIVATA

POSSIBILI DIFESE

- UTILIZZO DI ALGORITMI CON TEMPI DI CALCOLO COSTANTI
  - NON SEMPRE PRATICO
  - NON SONO POSSIBILI OTTIMIZZAZIONI
- UTILIZZO DI ALGORITMI CHE AGGIUNGONO RITARDI CASUALI
  - OVER-HEAD
  - NON SONO POSSIBILI OTTIMIZZAZIONI
- RSA BLINDING

RSA BLINDING

- SI CALCOLA UN NUMERO RANDOM r
- SI COMPUTA $S' = (r^e M)^d mod(N)$
- SI CONSIDERA L'INVERSO DI r, r^{-1}
- SI CREA LA FIRMA ESEGUENDO IL CALCOLO $r^{-1} S' = M^d mod(N)$

IL TEMPO IMPIEGATO PER FIRMARE IL MESSAGGIO NON È PIÙ CORRELATO AL MESSAGGIO IN INPUT, QUINDI NON È POSSIBILE OTTENERE INFORMAZIONI

CONCLUSIONI

ATTACCHI COME IL TIMING ATTACK CI DICONO CHE, ANCHE SE UN SISTEMA È MATEMATICAMENTE FORTE, IN PRATICA, LA SICUREZZA DIPENDE ANCHE DALLA MODALITÀ DI IMPLEMENTAZIONE DEL SISTEMA.

LA CRITTOGRAFIA NON DEVE ESSERE ESAMINATA IN MANIERA ISOLATA. LA PROGETTAZIONE DI UN SISTEMA SICURO DOVREBBE COMPRENDERE OGNI ASPETTO, CRITTOGRAFICO E NON. SI PRESUME CHE UN AGGRESSORE ATTACCA, SEMPRE, L'ANELLO PIÙ DEBOLE DI UN SISTEMA.

FINE

GRAZIE