L'agoritmo RSA

Gregorio D'Agostino

29 Marzo 2021

Esercizi sulle potenze in $\mathbb{Z}_n^*$

Generalità sulla criptografia moderna

L'agoritmo RSA

Esercizi per la prossima lezione

Verifica proprietà ed esercizi alla lavagna.

- Esercizi Tabelle pitagoriche e potenze in $\mathbb{Z}_n^*$.

Verifica proprietà ed esercizi alla lavagna.

- Esercizi Tabelle pitagoriche e potenze in $\mathbb{Z}_n^*$.
- Isomorfismi interni. Calcolo dell'invariate.

Verifica proprietà ed esercizi alla lavagna.

- Esercizi Tabelle pitagoriche e potenze in $\mathbb{Z}_n^*$.
- Isomorfismi interni. Calcolo dell'invariate.
- Correzione esercizio sulla Primalità cinese. I primi tre numeri non primi che passano il vaglio cinese sono 341=(11) (31), 561= 3 (187) e 645 = 3 (215). 1,7% di errore.

Verifica proprietà ed esercizi alla lavagna.

- Esercizi Tabelle pitagoriche e potenze in $\mathbb{Z}_n^*$.
- Isomorfismi interni. Calcolo dell'invariate.
- Correzione esercizio sulla Primalità cinese. I primi tre numeri non primi che passano il vaglio cinese sono 341=(11) (31), 561= 3 (187) e 645 = 3 (215). 1,7% di errore.
- Correzione esercizi sui sistemi diofantei.

Pricipi della criptografia moderna

- La crittazione moderna si basa sul principio che le informazioni possono essere intercettate e che bisogna trovare un meccanismo (algoritmo), noto a tutti ameno di una chiave, mediante il quale, la forma in cui esse vengono acquisite sia inutilizzabile. Questo meccanismo è la cifratura.

Pricipi della criptografia moderna

- La crittazione moderna si basa sul principio che le informazioni possono essere intercettate e che bisogna trovare un meccanismo (algoritmo), noto a tutti ameno di una chiave, mediante il quale, la forma in cui esse vengono acquisite sia inutilizzabile. Questo meccanismo è la cifratura.
- La cifratura consiste nel trasformare i dati in una forma equivalente, ma incomprensibile o indecifrabile in un assegnato lasso di tempo anche avvalendosi dei mezzi di calcolo esistenti più avanzati. Per semplicità supporremo che l'informazione da proteggere sia rappresentabile tramite un numero m (messaggio). Abbiamo già visto esempi di cifratura numerica di testi. Il testo cifrato sarà c:

$$c = f(m).$$

Proprietà della cifratura - cont

- La cifratura è dunque una applicazione (funzione) da uno spazio numerico in se.

Proprietà della cifratura - cont

- La cifratura è dunque una applicazione (funzione) da uno spazio numerico in se.
- L'applicazione f dipende parametricamente da una chiave k:

$$c = c_k = f(m) = f_k(m).$$

la funzione f è nota a tutti, ma k è conosciuta solo al cifratore.

Algoritmi ingannevoli

- Una spia osserva l'ingresso di un accampamento

Algoritmi ingannevoli

- Una spia osserva l'ingresso di un accampamento
- La sentinella dice ad uno che vuole entrare: "altolà 12".

Algoritmi ingannevoli

- Una spia osserva l'ingresso di un accampamento
- La sentinella dice ad uno che vuole entrare: "altolà 12".
- Quello risponde 6 ed entra.

Algoritmi ingannevoli

- Una spia osserva l'ingresso di un accampamento
- La sentinella dice ad uno che vuole entrare: "altolà 12".
- Quello risponde 6 ed entra.
- Poi arriva un altro: "altolà 10".

Algoritmi ingannevoli

- Una spia osserva l'ingresso di un accampamento
- La sentinella dice ad uno che vuole entrare: "altolà 12".
- Quello risponde 6 ed entra.
- Poi arriva un altro: "altolà 10".
- Quello risponde 5 ed entra.

Algoritmi ingannevoli

- Una spia osserva l'ingresso di un accampamento
- La sentinella dice ad uno che vuole entrare: "altolà 12".
- Quello risponde 6 ed entra.
- Poi arriva un altro: "altolà 10".
- Quello risponde 5 ed entra.
- Poi arriva un altro: "altolà 8".

Algoritmi ingannevoli

- Una spia osserva l'ingresso di un accampamento
- La sentinella dice ad uno che vuole entrare: "altolà 12".
- Quello risponde 6 ed entra.
- Poi arriva un altro: "altolà 10".
- Quello risponde 5 ed entra.
- Poi arriva un altro: "altolà 8".
- Quello risponde 4 ed entra.

Algoritmi ingannevoli

- Una spia osserva l'ingresso di un accampamento
- La sentinella dice ad uno che vuole entrare: "altolà 12".
- Quello risponde 6 ed entra.
- Poi arriva un altro: "altolà 10".
- Quello risponde 5 ed entra.
- Poi arriva un altro: "altolà 8".
- Quello risponde 4 ed entra.
- Poi arriva un altro: "altolà 6".

Algoritmi ingannevoli

- Una spia osserva l'ingresso di un accampamento
- La sentinella dice ad uno che vuole entrare: "altolà 12".
- Quello risponde 6 ed entra.
- Poi arriva un altro: "altolà 10".
- Quello risponde 5 ed entra.
- Poi arriva un altro: "altolà 8".
- Quello risponde 4 ed entra.
- Poi arriva un altro: "altolà 6".
- Quello risponde 3 ed entra.

Algoritmi ingannevoli

- Una spia osserva l'ingresso di un accampamento
- La sentinella dice ad uno che vuole entrare: "altolà 12".
- Quello risponde 6 ed entra.
- Poi arriva un altro: "altolà 10".
- Quello risponde 5 ed entra.
- Poi arriva un altro: "altolà 8".
- Quello risponde 4 ed entra.
- Poi arriva un altro: "altolà 6".
- Quello risponde 3 ed entra.
- Poi prova la spia: "altolà 4".

Algoritmi ingannevoli

- Una spia osserva l'ingresso di un accampamento
- La sentinella dice ad uno che vuole entrare: "altolà 12".
- Quello risponde 6 ed entra.
- Poi arriva un altro: "altolà 10".
- Quello risponde 5 ed entra.
- Poi arriva un altro: "altolà 8".
- Quello risponde 4 ed entra.
- Poi arriva un altro: "altolà 6".
- Quello risponde 3 ed entra.
- Poi prova la spia: "altolà 4".
- La spia risponde 2 e viene fucilato...

Proprietà della cifratura - cont

- Le informazioni devono essere utilizzabili dai soggetti autorizzati, dunque deve esistere un metodo per trasformare i dati espressi nella forma cifrata in dati in dati leggibili. Questo metodo è l'algoritmo di decifrazione:

$$\exists g : t = g(c);\ t = g(f(m)) = m$$

Proprietà della cifratura - cont

- Le informazioni devono essere utilizzabili dai soggetti autorizzati, dunque deve esistere un metodo per trasformare i dati espressi nella forma cifrata in dati in dati leggibili. Questo metodo è l'algoritmo di decifrazione:

$$\exists g : t = g(c);\ t = g(f(m)) = m$$

- Anche l'applicazione g è conosciuta a tutti ma anch'essa dipende dalla chiave.

$$\exists g = g_k : t = g_k(c_k);\ t = g_k(f_k(m)) = m$$

Proprietà della cifratura - cont

- Le informazioni devono essere utilizzabili dai soggetti autorizzati, dunque deve esistere un metodo per trasformare i dati espressi nella forma cifrata in dati in dati leggibili. Questo metodo è l'algoritmo di decifrazione:

$$\exists g : t = g(c);\ t = g(f(m)) = m$$

- Anche l'applicazione g è conosciuta a tutti ma anch'essa dipende dalla chiave.

$$\exists g = g_k : t = g_k(c_k);\ t = g_k(f_k(m)) = m$$

- La g è una procedura per il calcolo della funzione inversa di f, cioè un algoritmo che dato un testo cifrato restituisce l'originale in chiaro.

Proprietà della cifratura - cont

- Le informazioni devono essere utilizzabili dai soggetti autorizzati, dunque deve esistere un metodo per trasformare i dati espressi nella forma cifrata in dati in dati leggibili. Questo metodo è l'algoritmo di decifrazione:

$$\exists g : t = g(c);\ t = g(f(m)) = m$$

- Anche l'applicazione g è conosciuta a tutti ma anch'essa dipende dalla chiave.

$$\exists g = g_k : t = g_k(c_k);\ t = g_k(f_k(m)) = m$$

- La g è una procedura per il calcolo della funzione inversa di f, cioè un algoritmo che dato un testo cifrato restituisce l'originale in chiaro.
- Anche la $g_k()$ deve essere computabile facilmente (cioè in un tempo breve con le risorse di calcolo disponibili).

Proprietà della cifratura

- L'applicazione f deve essere iniettiva. A testi diversi devono corrispondere crittogrammi diversi. Altrimenti nessuno, nemmeno il cifratore, potrebbe decifrare univocamente il contenuto.

Proprietà della cifratura

- L'applicazione f deve essere iniettiva. A testi diversi devono corrispondere crittogrammi diversi. Altrimenti nessuno, nemmeno il cifratore, potrebbe decifrare univocamente il contenuto.
- L'applicazione f tuttavia può essere polidroma, cioè condurre a più cifrature equivalenti tra loro (la cui decifrazione porta allo stesso messaggio originale). L'esempio più eclatante è dato dal dna: le sequenze di 3 basi azotate (AGCT) corrispondono solo a 20 aminoacidi (blocchi proteine).

Proprietà della cifratura

- L'applicazione f deve essere iniettiva. A testi diversi devono corrispondere crittogrammi diversi. Altrimenti nessuno, nemmeno il cifratore, potrebbe decifrare univocamente il contenuto.
- L'applicazione f tuttavia può essere polidroma, cioè condurre a più cifrature equivalenti tra loro (la cui decifrazione porta allo stesso messaggio originale). L'esempio più eclatante è dato dal dna: le sequenze di 3 basi azotate (AGCT) corrispondono solo a 20 aminoacidi (blocchi proteine).
- L'applicazione g di "decifrazione" deve invece essere una funzione ad un solo valore, ma può non essere iniettiva: le diverse codifiche ammesse per lo stesso messaggio devono portare allo stesso valore.

Proprietà della cifratura

- L'applicazione f deve essere iniettiva. A testi diversi devono corrispondere crittogrammi diversi. Altrimenti nessuno, nemmeno il cifratore, potrebbe decifrare univocamente il contenuto.
- L'applicazione f tuttavia può essere polidroma, cioè condurre a più cifrature equivalenti tra loro (la cui decifrazione porta allo stesso messaggio originale). L'esempio più eclatante è dato dal dna: le sequenze di 3 basi azotate (AGCT) corrispondono solo a 20 aminoacidi (blocchi proteine).
- L'applicazione g di "decifrazione" deve invece essere una funzione ad un solo valore, ma può non essere iniettiva: le diverse codifiche ammesse per lo stesso messaggio devono portare allo stesso valore.
- Se l'algoritmo di cifratura è universale (cioè in grado di cifrare qualunque testo), il codominio di g deve essere tutto lo spazio dei testi cifrabili e g deve essere suriettiva.

Il problema della decrittazione

- Spesso si utilizza lo stesso algoritmo di cifratura e la stessa chiave per un certo periodo di tempo o per una attività specifica ripetitiva. Possono verificarsi diverse condizioni:

Il problema della decrittazione

- Spesso si utilizza lo stesso algoritmo di cifratura e la stessa chiave per un certo periodo di tempo o per una attività specifica ripetitiva. Possono verificarsi diverse condizioni:
- Divengono disponibili a tutti o agli attaccanti alcuni testi cifrati (crittogrammi) di cui non si conosce il testo sorgente. Si attua dunque una vulnerabilità rispetto ad una minaccia di tipo "Cipher text attack" (decrittazione di crittogrammi ignoti). In questo caso il primo passo per l'attaccante e decifrare i messaggi.

Il problema della decrittazione

- Spesso si utilizza lo stesso algoritmo di cifratura e la stessa chiave per un certo periodo di tempo o per una attività specifica ripetitiva. Possono verificarsi diverse condizioni:
- Divengono disponibili a tutti o agli attaccanti alcuni testi cifrati (crittogrammi) di cui non si conosce il testo sorgente. Si attua dunque una vulnerabilità rispetto ad una minaccia di tipo "Cipher text attack" (decrittazione di crittogrammi ignoti). In questo caso il primo passo per l'attaccante e decifrare i messaggi.
- Divengono disponibili a tutti o agli attaccanti alcuni crittogrammi di cui si conosce il testo sorgente. Si attua dunque una vulnerabilità rispetto ad un attacco di tipo "Known Plain text attack" (deduzione della chiave da crittogrammi noti). La finalità in questo caso è scoprire l'algoritmo di cifratura (e la chiave) o, in subordine, decifrare altri messaggi cifrati o una loro parte.

Il problema della decrittazione - cont

- Diviene disponibile una macchina che per ogni testo sorgente fornisce il testo cifrato (esempio storico il codice Enigma). Si attua dunque una vulnerabilità rispetto ad una minaccia di tipo "Chosen Plain text attack". La finalità in questo caso è trovare una formalizzazione dell'algoritmo di cifratura, cioè la chiave o decifrare altri messaggi cifrati.

Il problema della decrittazione - cont

- Diviene disponibile una macchina che per ogni testo sorgente fornisce il testo cifrato (esempio storico il codice Enigma). Si attua dunque una vulnerabilità rispetto ad una minaccia di tipo "Chosen Plain text attack". La finalità in questo caso è trovare una formalizzazione dell'algoritmo di cifratura, cioè la chiave o decifrare altri messaggi cifrati.
- In ognuno dei casi precedenti l'algoritmo di cifratura può essere noto, ma non la chiave. Nel caso più comune si ha la massima vulnerabilità del sistema: l'algoritmo è noto e il potenziale attaccante dispone di uno strumento automatizzato (tipicamente un codice eseguibile) per cifrare tutti i messaggi che desidera.
  La sicurezza informatica moderna richiede la protezione dei dati anche in quest'ultimo caso.

Il problema della decrittazione - cont

- Diviene disponibile una macchina che per ogni testo sorgente fornisce il testo cifrato (esempio storico il codice Enigma). Si attua dunque una vulnerabilità rispetto ad una minaccia di tipo "Chosen Plain text attack". La finalità in questo caso è trovare una formalizzazione dell'algoritmo di cifratura, cioè la chiave o decifrare altri messaggi cifrati.
- In ognuno dei casi precedenti l'algoritmo di cifratura può essere noto, ma non la chiave. Nel caso più comune si ha la massima vulnerabilità del sistema: l'algoritmo è noto e il potenziale attaccante dispone di uno strumento automatizzato (tipicamente un codice eseguibile) per cifrare tutti i messaggi che desidera.
  La sicurezza informatica moderna richiede la protezione dei dati anche in quest'ultimo caso.
- In questo caso la complessità della decrittazione è data solo dalla complessità della chiave, cioè dalla cardinalità dello spazio delle chiavi.

Crittografia a chiave pubblica

- Diffie & Helman e autonomamente Merkle nel 1976 introdussero il concetto di "Crittografia a chiave pubblica". In cui volutamente ci si mette nelle condizioni di massima vulnerabilità fornendo una algoritmo (e la chiave) per cifrare i messaggi, ma solo chi possiede una seconda chiave segreta può decifrare in un tempo breve.

Crittografia a chiave pubblica

- Diffie & Helman e autonomamente Merkle nel 1976 introdussero il concetto di "Crittografia a chiave pubblica". In cui volutamente ci si mette nelle condizioni di massima vulnerabilità fornendo una algoritmo (e la chiave) per cifrare i messaggi, ma solo chi possiede una seconda chiave segreta può decifrare in un tempo breve.
- Gli algorittimi f e g sono noti a tutti e dipendono entrambi da chiavi. La chiave di f è detta "pubblica" ed nota a tutti , mentre la chiave α di g (che dipende da k, $\alpha = \alpha(k)$) è ignota e, pertanto è detta "privata".

$$\forall t : t \equiv g_\alpha(f_k(t));$$

Crittografia a chiave pubblica

- Diffie & Helman e autonomamente Merkle nel 1976 introdussero il concetto di "Crittografia a chiave pubblica". In cui volutamente ci si mette nelle condizioni di massima vulnerabilità fornendo una algoritmo (e la chiave) per cifrare i messaggi, ma solo chi possiede una seconda chiave segreta può decifrare in un tempo breve.
- Gli algorittimi f e g sono noti a tutti e dipendono entrambi da chiavi. La chiave di f è detta "pubblica" ed nota a tutti , mentre la chiave α di g (che dipende da k, $\alpha = \alpha(k)$) è ignota e, pertanto è detta "privata".

$$\forall t : t \equiv g_\alpha(f_k(t));$$

- In molti casi f e g commutano tra loro, quindi:

$$\forall t : t \equiv f_k(g_\alpha(t)).$$

Principali usi della crittografia a chiavi asimmetriche

- Condivisione riservata di informazioni: Chiunque può usare la chiave pubblica di A per dare informazioni solo a lei/lui in forma cifrata. I dati possono essere collocati in domini pubblici non protetti.

Principali usi della crittografia a chiavi asimmetriche

- Condivisione riservata di informazioni: Chiunque può usare la chiave pubblica di A per dare informazioni solo a lei/lui in forma cifrata. I dati possono essere collocati in domini pubblici non protetti.
- Firma digitale di un testo: Cifrando con la propria chiave privata, chiunque può garantire il mittente ovvero l'autore di un testo. [Vedremo che in realtà non si critta tutto ma solo una opportuna funzione].

Principali usi della crittografia a chiavi asimmetriche

- Condivisione riservata di informazioni: Chiunque può usare la chiave pubblica di A per dare informazioni solo a lei/lui in forma cifrata. I dati possono essere collocati in domini pubblici non protetti.
- Firma digitale di un testo: Cifrando con la propria chiave privata, chiunque può garantire il mittente ovvero l'autore di un testo. [Vedremo che in realtà non si critta tutto ma solo una opportuna funzione].
- Comunicazione pubblica riservata: Scambio di messaggi segreti e firmati su canali (o reti) di comunicazione aperte (non protette). Adesso Whatsapp usa la "End to end cryptography" che è basata esattamente sulla cifratura a chiave simmetrica.

Esempio di comunicazione firmata e riservata

- Alessandra invia il messaggio m a Bruno con riservatezza e certezza di mittente. Avvalendosi della crittografia a chiavi asimmetriche esegue questi passi:

Esempio di comunicazione firmata e riservata

- Alessandra invia il messaggio m a Bruno con riservatezza e certezza di mittente. Avvalendosi della crittografia a chiavi asimmetriche esegue questi passi:
- cifra il messaggio con la sua chiave privata α_A:

$$c_A = g_{\alpha_A}(m);$$

Esempio di comunicazione firmata e riservata

- Alessandra invia il messaggio m a Bruno con riservatezza e certezza di mittente. Avvalendosi della crittografia a chiavi asimmetriche esegue questi passi:
- cifra il messaggio con la sua chiave privata α_A:

$$c_A = g_{\alpha_A}(m);$$

- poi lo ri-cifra con la chiave pubblica di Bruno k_B:

$$c = f_{k_B}(c_A);$$

Esempio di comunicazione firmata e riservata

- Alessandra invia il messaggio m a Bruno con riservatezza e certezza di mittente. Avvalendosi della crittografia a chiavi asimmetriche esegue questi passi:
- cifra il messaggio con la sua chiave privata α_A:

$$c_A = g_{\alpha_A}(m);$$

- poi lo ri-cifra con la chiave pubblica di Bruno k_B:

$$c = f_{k_B}(c_A);$$

- poi lo invia pubblicamente (su rete non protetta) a Bruno.

Esempio di comunicazione firmata e riservata

- Alessandra invia il messaggio m a Bruno con riservatezza e certezza di mittente. Avvalendosi della crittografia a chiavi asimmetriche esegue questi passi:
- cifra il messaggio con la sua chiave privata α_A:

$$c_A = g_{\alpha_A}(m);$$

- poi lo ri-cifra con la chiave pubblica di Bruno k_B:

$$c = f_{k_B}(c_A);$$

- poi lo invia pubblicamente (su rete non protetta) a Bruno.
- Bruno riceve c e lo decifra con la sua chiave privata:

$$c_A = g_{\alpha_B}(c);$$

Esempio di comunicazione firmata e riservata

- Alessandra invia il messaggio m a Bruno con riservatezza e certezza di mittente. Avvalendosi della crittografia a chiavi asimmetriche esegue questi passi:
- cifra il messaggio con la sua chiave privata α_A:

$$c_A = g_{\alpha_A}(m);$$

- poi lo ri-cifra con la chiave pubblica di Bruno k_B:

$$c = f_{k_B}(c_A);$$

- poi lo invia pubblicamente (su rete non protetta) a Bruno.
- Bruno riceve c e lo decifra con la sua chiave privata:

$$c_A = g_{\alpha_B}(c);$$

- e poi lo ridecifra con la chiave pubblica di Alessandra:

$$t = f_{k_A}(c_A) \equiv m.$$

Esempio di comunicazione firmata e riservata

- Alessandra invia il messaggio m a Bruno con riservatezza e certezza di mittente. Avvalendosi della crittografia a chiavi asimmetriche esegue questi passi:
- cifra il messaggio con la sua chiave privata α_A:

$$c_A = g_{\alpha_A}(m);$$

- poi lo ri-cifra con la chiave pubblica di Bruno k_B:

$$c = f_{k_B}(c_A);$$

- poi lo invia pubblicamente (su rete non protetta) a Bruno.
- Bruno riceve c e lo decifra con la sua chiave privata:

$$c_A = g_{\alpha_B}(c);$$

- e poi lo ridecifra con la chiave pubblica di Alessandra:

$$t = f_{k_A}(c_A) \equiv m.$$

- La povera Deborah (rivale di Alessandra) non può fare nulla per modificare o leggere il messaggio...

I cavalieri che fecero l'impresa

- Ron Rivest, Adi Shamir e Leonard Adleman, nel 1978 trovarono un modo elegante per realizzare la crittografia a chiave asimmetrica. Basandosi sul teorema di Eulero e sulle proprietà degli anelli.

I cavalieri che fecero l'impresa

- Ron Rivest, Adi Shamir e Leonard Adleman, nel 1978 trovarono un modo elegante per realizzare la crittografia a chiave asimmetrica. Basandosi sul teorema di Eulero e sulle proprietà degli anelli.
- Come funzione di cifratura con chiave pubblica k scelsero l'esponenziale in un anello con modulo il prodotto di due numeri primi grandi $n = pq$:

$$c_k = m^k \ (mod \ n).$$

I cavalieri che fecero l'impresa

- Ron Rivest, Adi Shamir e Leonard Adleman, nel 1978 trovarono un modo elegante per realizzare la crittografia a chiave asimmetrica. Basandosi sul teorema di Eulero e sulle proprietà degli anelli.
- Come funzione di cifratura con chiave pubblica k scelsero l'esponenziale in un anello con modulo il prodotto di due numeri primi grandi $n = pq$:

$$c_k = m^k \ (mod \ n).$$

- Il testo segreto è m (con $m < n$).

I cavalieri che fecero l'impresa

- Ron Rivest, Adi Shamir e Leonard Adleman, nel 1978 trovarono un modo elegante per realizzare la crittografia a chiave asimmetrica. Basandosi sul teorema di Eulero e sulle proprietà degli anelli.
- Come funzione di cifratura con chiave pubblica k scelsero l'esponenziale in un anello con modulo il prodotto di due numeri primi grandi $n = pq$:

$$c_k = m^k \ (mod \ n).$$

- Il testo segreto è m (con $m < n$).
- Sono noti a tutti: l'algoritmo di cifratura, n e k (un numero primo con n).

I cavalieri che fecero l'impresa

- Ron Rivest, Adi Shamir e Leonard Adleman, nel 1978 trovarono un modo elegante per realizzare la crittografia a chiave asimmetrica. Basandosi sul teorema di Eulero e sulle proprietà degli anelli.
- Come funzione di cifratura con chiave pubblica k scelsero l'esponenziale in un anello con modulo il prodotto di due numeri primi grandi $n = pq$:

$$c_k = m^k \ (mod \ n).$$

- Il testo segreto è m (con $m < n$).
- Sono noti a tutti: l'algoritmo di cifratura, n e k (un numero primo con n).
- La chiave segreta è p (o q perché n=pq).

I cavalieri che fecero l'impresa

- Ron Rivest, Adi Shamir e Leonard Adleman, nel 1978 trovarono un modo elegante per realizzare la crittografia a chiave asimmetrica. Basandosi sul teorema di Eulero e sulle proprietà degli anelli.
- Come funzione di cifratura con chiave pubblica k scelsero l'esponenziale in un anello con modulo il prodotto di due numeri primi grandi $n = pq$:

$$c_k = m^k \ (mod \ n).$$

- Il testo segreto è m (con $m < n$).
- Sono noti a tutti: l'algoritmo di cifratura, n e k (un numero primo con n).
- La chiave segreta è p (o q perché n=pq).
- La funzione di decifrazione è g:

$$g(c_k) \equiv m \ (mod \ n).$$

Funzione di decifrazione

- La funzione g deve ridare il messaggio qualunque sia il testo originario m. La cerchiamo sotto forma di una potenza ad un esponente α ignoto:

$$\forall m : m = g(c_k) = (c_k)^{\alpha} \equiv m \, (mod \ n).$$

Funzione di decifrazione

- La funzione g deve ridare il messaggio qualunque sia il testo originario m. La cerchiamo sotto forma di una potenza ad un esponente α ignoto:

$$\forall m : m = g(c_k) = (c_k)^{\alpha} \equiv m \ (mod \ n).$$

- $$\forall m : m = g(c_k) = (c_k)^{\alpha} = m^{k\alpha} \equiv m \ (mod \ n);$$

  cioè:

$$m^{k\alpha} \equiv m \ (mod \ n).$$

Funzione di decifrazione -cont

- Dal teorema di Eulero sappiamo che

$$m^{\phi(n)+1} \equiv m \ (mod \ n).$$

e quindi per qualsiasi intero l anche

$$\forall l : m^{l\phi(n)+1} \equiv m \ (mod \ n).$$

Se si trova un α che soddisfi l'equazione per un intero l:

$$l\phi(n) + 1 = \alpha \cdot k;$$

il problema è risolto.

Funzione di decifrazione -cont

- Dal teorema di Eulero sappiamo che

$$m^{\phi(n)+1} \equiv m \ (mod \ n).$$

e quindi per qualsiasi intero l anche

$$\forall l : m^{l\phi(n)+1} \equiv m \ (mod \ n).$$

Se si trova un α che soddisfi l'equazione per un intero l:

$$l\phi(n) + 1 = \alpha \cdot k;$$

il problema è risolto.

- Quindi la chiave per risolvere il problema è trovare α: l'inverso di k modulo $\phi(n) = \phi(pq) = (p-1)(q-1)$:

$$\alpha \cdot k \equiv 1 \ (mod \ \phi(n));$$

Qual è il problema del decifratore?

- Deve risolvere l'equazione diofantea:

$$\alpha \cdot k \equiv 1 \ (mod \ \phi(n));$$

cioè:

$$\alpha \cdot k \equiv 1 \ (mod \ (p-1) \cdot (q-1)).$$

Qual è il problema del decifratore?

- Deve risolvere l'equazione diofantea:

$$\alpha \cdot k \equiv 1 \ (mod \ \phi(n));$$

cioè:

$$\alpha \cdot k \equiv 1 \ (mod \ (p-1) \cdot (q-1)).$$

- Questa equivale ad sistema perché entrambi $p-1$ e $q-1$ sono pari e quindi ϕ è divisibile per un multiplo di quattro 2^m. $\phi = 2^m \cdot \phi'$.

$$\begin{cases} \alpha \cdot k & \equiv & 1 & (mod & \phi'); \\ \alpha \cdot k & \equiv & 1 & (mod & 2^m). \end{cases}$$

Qual è il problema del decifratore?

- Deve risolvere l'equazione diofantea:

$$\alpha \cdot k \equiv 1 \ (mod \ \phi(n));$$

cioè:

$$\alpha \cdot k \equiv 1 \ (mod \ (p-1) \cdot (q-1)).$$

- Questa equivale ad sistema perché entrambi $p-1$ e $q-1$ sono pari e quindi ϕ è divisibile per un multiplo di quattro 2^m. $\phi = 2^m \cdot \phi'$.

$$\begin{cases} \alpha \cdot k & \equiv & 1 & (mod & \phi'); \\ \alpha \cdot k & \equiv & 1 & (mod & 2^m). \end{cases}$$

- Siccome ϕ' è fattorizzato in almeno due fattori, il decifratore deve risolvere (una volta sola per ogni chiave pubblica che usa) un sistema diofanteo con variabili intere minori del massimo tra p e q. Vedremo che i problema della ricerca di α può essere leggermente semplificato.

Qual è il problema del decrittatore cioè dell'attaccante?

- Nel caso di RSA si tratta di "chosen text attack", cioè l'attaccante dispone di una macchina in grado di cifrare qualsiasi testo scelto.

Qual è il problema del decrittatore cioè dell'attaccante?

- Nel caso di RSA si tratta di "chosen text attack", cioè l'attaccante dispone di una macchina in grado di cifrare qualsiasi testo scelto.
- Conosce anche l'algoritmo di decifrazione, ma non ne conosce la chiave α

Qual è il problema del decrittatore cioè dell'attaccante?

- Nel caso di RSA si tratta di "chosen text attack", cioè l'attaccante dispone di una macchina in grado di cifrare qualsiasi testo scelto.
- Conosce anche l'algoritmo di decifrazione, ma non ne conosce la chiave α
- Potrebbe cercare a caso ('brute force' ovvero ispezione casuale) delle chiavi per vedere se funzionano, ma lo spazio della chiavi è troppo grande. Quindi servono metodi alternativi per trovare α o decomporre $n = pq$.

Qual strategie può seguire l'attaccante?

- Ha diverse strade: la prima consiste nel decomporre n in fattori e trovare p e q. In tal modo si riconduce al problema (semplice) del decifratore.

Qual strategie può seguire l'attaccante?

- Ha diverse strade: la prima consiste nel decomporre n in fattori e trovare p e q. In tal modo si riconduce al problema (semplice) del decifratore.
- Alternativamente può trovare direttamente una chiave α.

Qual strategie può seguire l'attaccante?

- Ha diverse strade: la prima consiste nel decomporre n in fattori e trovare p e q. In tal modo si riconduce al problema (semplice) del decifratore.
- Alternativamente può trovare direttamente una chiave α.
- In entrambi i casi deve affrontare un problema di interi tra 1 ed n.

Qual strategie può seguire l'attaccante?

- Ha diverse strade: la prima consiste nel decomporre n in fattori e trovare p e q. In tal modo si riconduce al problema (semplice) del decifratore.
- Alternativamente può trovare direttamente una chiave α.
- In entrambi i casi deve affrontare un problema di interi tra 1 ed n.
- Vedremo quali sono i problemi in entrambi i casi. Il punto fondamentale è che le possibili chiavi p, q o α variano in una spazio di dimensione n; però spesso l'ispezione si riduce a $\sim min(p, q) \sim \sqrt{n}$ valori. Se n è un numero a 256bit, la sua radice quadrata ha 128 bit.
  $2^{128} \sim 2^8 \cdot (2^{10})^12 \sim 256 \cdot 1024^{12} \sim 3 \cdot 10^{38}$. La macchina più potente attualmente non arriva al petafloap=10^{15} operazioni al secondo... Il metodo della forza bruta, cioè l'ispezione esaustiva delle chiavi sembra escluso: impiegherebbe $10^{16} anni$, milioni di volte la vita dell'universo...

Problema del cifratore

- Deve trovare due numeri primi diversi (poi vedremo abbastanza distanti) grandi ad esempio 2^{128} bit.

Problema del cifratore

- Deve trovare due numeri primi diversi (poi vedremo abbastanza distanti) grandi ad esempio 2^{128} bit.
- I due numeri p e q devono essere presi a caso da un insieme molto grande di chiavi altrimenti il decrittatore cerca di riprodurre i criteri di scelta della chiave.:

Problema del cifratore

- Deve trovare due numeri primi diversi (poi vedremo abbastanza distanti) grandi ad esempio 2^{128} bit.
- I due numeri p e q devono essere presi a caso da un insieme molto grande di chiavi altrimenti il decrittatore cerca di riprodurre i criteri di scelta della chiave.:
- Deve trovare un numero k primo con n e con qualche altra semplice proprietà (questo non è difficile).

Esercizi

- Problema della spia.
  Quale tipo di attacco ha perpetrato?
  Qual è un algoritmo semplice per il problema della spia?
  Suggerimento la spia avrebbe dovuto rispondere sette.
  La soluzione proposta è unica?

Esercizi

- Problema della spia.
  Quale tipo di attacco ha perpetrato?
  Qual è un algoritmo semplice per il problema della spia?
  Suggerimento la spia avrebbe dovuto rispondere sette.
  La soluzione proposta è unica?
- Scrivere un programma Octave che fissata la base n=91=7x13 calcoli i periodi (cioè gli ordini) di tutti inumeri b con $1 < b < n$. Si distingua tra il caso b primo con n ed il caso b divisore dello zero (cioè non coprimo con n).
  Usare l'algoritmo di euclide per derimere i due casi.
  Nel primo caso si esce quando $b^k = 1$; nel secondo quando $b^k = b$ oppure, (ma per n=91 non capita), $b^k = 0$.