ТЕОРИЈА НА БРОЕВИ И КРИПТОСИСТЕМИ

Сашко Јанев
Огнен Спироски

Содржина

Прости броеви и факторизација

Евклидов алгоритам за Најголем Заеднички Делител (НЗД)

Криптосистеми со јавен клуч

RSA алгоритам

Својства и примена на алгоритмите за криптирање

Прости броеви

Основна теорема на аритметиката

- Секој позитивен број поголем од 1 може да биде претставен на *единствен* начин како производ од прости броеви помали од него

Генерирање на прости броеви е потребно за алгоритми со јавен клуч

Тестирање на својство на прост број:

- Детерминистички, пробабилистички, хеуристички

Факторизација

Разложување на еден објект во производ од алгебарски изрази.

Современите методи постигнуваат помеѓу полиномно и експоненцијално време, во областа наречена под-експоненцијално време

Dark Age методи:

- Trial division
- p-1 метод
- p+1 метод
- Pollard rho метод

Современи методи:

- Continued Fraction Method
- Quadratic Sieve
- Elliptic Curve Method
- Number Field Sieve

Евклидов алгоритам

Се базира врз барање на Најголем Заеднички Делител на два броеви

ТЕОРЕМА: За било кои два ненегативни цели броеви a и b, НЗД(a,b)=НЗД(b, a mod b)

Рекурзивен алгоритам:

```
Euclid(a,b)
If b==0
    Return a
Else return Euclid(b, a mod b)
```

Својства на Евклидов алгоритам

Се користи за пресметување на операција делење во модуларна аритметика

Проширената верзија на Евклидов алгоритам пресметува дополнителни информиции и е корисна за наоѓање модуларни мултипликативни инверзии

Основа на криптографски алгоритми како RSA, применет за решавање:

- Модуларно линеарни равенства
  - $ax = b \ (mod\ n)$, каде $a > 0$ и $n > 0$

Криптосистеми со Јавен Клуч

Вовед

Првиот јавно објавен систем е на Diffie-Hellman во 1976. Во 1978 објавен е RSA (Rivest, Shamir, Adleman).

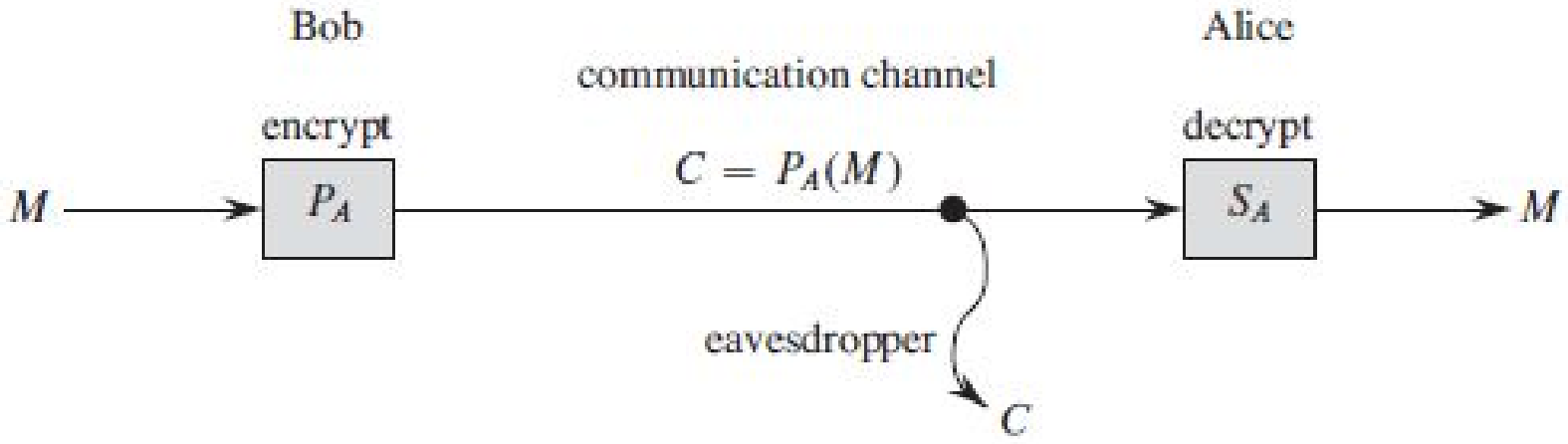
Се базира на пар клучеви - **јавен** и **таен клуч**.

Јавниот клуч се користи за криптирање, а тајниот за декриптирање.

Во криптосистемите со јавен клуч, јавниот клуч може слободно да се објави, додека тајниот клуч останува таен и тој го знае само оној за кого се наменети пораките.

Овозможува додавање на **дигитален потпис** на пораките

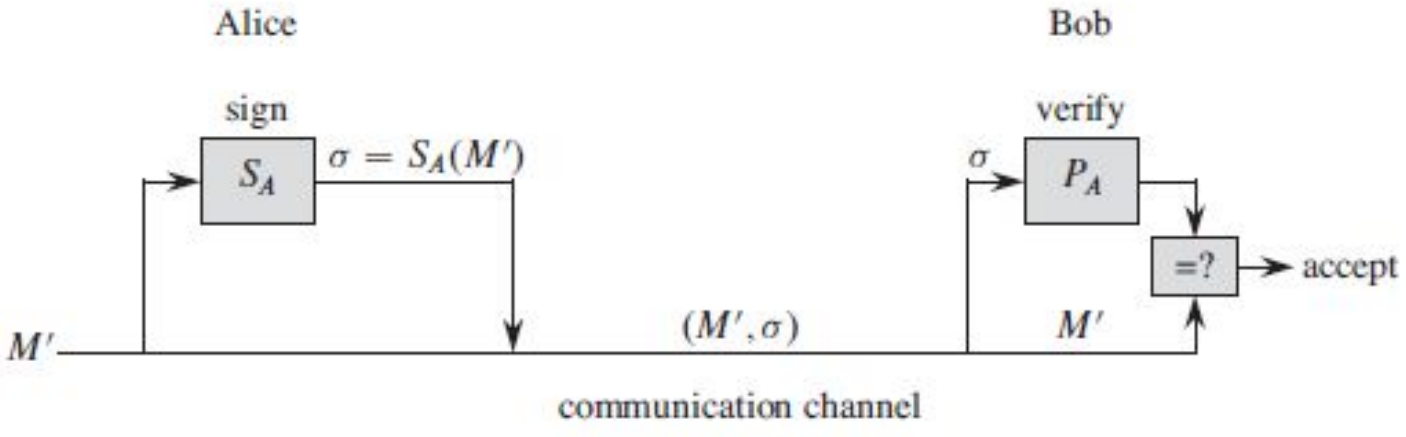
Енкрипција и Декрипција на податоци



$M = S_A(P_A(M))$

$M = P_A(S_A(M))$

Дигитални Потписи



Потпишаната порака со дигитален потпис може, но и не мора да биде енкриптирана.

RSA алгоритам

1. **Генерирање на клуч**
   1) избор на два прости броеви p и q со различна должина
   2) пресметување на производот R=p*q.
   3) пресметување на функцијата phi(R)=(p-1)*(q-1).
   4) избор на број S, каде 1 < S < phi(R) и НЗД(S, phi(R))=1.
   5) пресметување на бројот A= S^{-1} mod phi(R).
   6) Бројот A е тајниот клуч, додека пак парот (R, S) е јавниот клуч.
2. **Енкрипција**

$$E = M^S \bmod R$$

Криптиранта порака е пораката E, која Боб во оваа форма може да и ја прати на Алиса.

3. **Декрипција**

Кога Алис ќе ја добие енкриптираната порака E од Боб, таа пресметува:

$$D = E^A \bmod R$$

Добиениот текст D е всушност оргиналната порака M.

ElGammal алгоритам

Се заснова на проблемот на дискретен логаритам:

Ако p е голем прост број и ако a и b се познати цели броеви, тогаш x го наоѓаме од равенката:

$$a^x = b \pmod p$$

Не постои ефикасен брз метод за пресметување на овој проблем

За сигурност се потребни јаки случајни експоненти и прости броеви и долги клучеви над 1024 бита

Обично се користи во хибриден крипто-систем:

- Само за енкрипција на клуч од симетричен систем

Knapsack алгоритам

Измислен во 1978 од Merkle-Hellman и е пробиен од Shamir во 1984

Името на овој алгоритам произлегува од проблемот со ранец со одредена големина кој мора да се наполни со највредните предмети

Проблем во комбинаторна оптимизација: за дадено множество на предмети, секој со одредена тежина и вредност, да се одреди кои предмети ќе се вклучат во колекцијата така што вкупната тежина да биде помала или еднаква на дадениот лимит и вкупната вредност да биде што е можно поголема

Примена на алгоритми

RSA

Над 30 години примена!

TSL/SSL за online безбедност (HTTPS)

DRM - Digital Rights Management

Слободна имплементација, нема патенти

ElGammal

DSS (Digital Signature Standarts) - оставање на дигитални потписи

Open Source Free Libraries - Crypto ++ , CryptoLib, Python, Java Cryptix

GNU Privacy Guard software

PGP (Pretty Good Privacy)

Заклучок

Теоријата на броеви наоѓа секојдневна практична примена во дигитална комуникација и e-commerce преку криптографски системи со јавен клуч

Основа на главните протоколи за безбедност на Интернет

Безбедноста е добра онолку колку што е добар изборот на параметри:

- Подобрувања во процесорска моќ овозможија решавање на математичките проблеми во догледно време, при помали должини на клучевите
- Користете многу долги клучеви!