**Tema : Protocolul de semnatura Chaum-van Antwerpen**

**Partea teoretica**

**David Lee Chaum** (n. 1955) este un [informatician](https://en.wikipedia.org/wiki/Computer_scientist) și [criptograf](https://en.wikipedia.org/wiki/List_of_cryptographers" \o "Lista criptografilor) american . Este cunoscut ca un pionier în tehnologiile de conservare a criptografiei și a vieții private și este recunoscut pe larg ca inventatorul numerarului digital. Disertația sa din 1982 „Computer Systems Established, Mentenată și Încredere de Grupuri Suspicioase”  este prima propunere cunoscută pentru un protocol blockchain. Completat cu codul pentru a implementa protocolul, disertația lui Chaum a propus toate elementele, cu excepția unui blockchain, detaliate mai târziu în [cartea](https://en.wikipedia.org/wiki/Bitcoin" \o "Bitcoin) albă [Bitcoin](https://en.wikipedia.org/wiki/Bitcoin) .

El este cunoscut și pentru dezvoltarea [ecash](https://en.wikipedia.org/wiki/Ecash" \o "Ecash) , o aplicație electronică de numerar care își propune să păstreze anonimatul unui utilizator și inventează multe protocoale [criptografice](https://en.wikipedia.org/wiki/Cryptography" \o "Criptografie) precum [semnătura oarbă](https://en.wikipedia.org/wiki/Blind_signature" \o "Semnătura orb) , [rețelele mix](https://en.wikipedia.org/wiki/Mix_networks" \o "Mixează rețelele) și [protocolul criptografilor Dining](https://en.wikipedia.org/wiki/Dining_cryptographers_protocol" \o "Protocolul criptografilor de luat masa) . În 1995, compania sa [DigiCash](https://en.wikipedia.org/wiki/DigiCash" \o "DigiCash) , o corporație de [bani electronici](https://en.wikipedia.org/wiki/Digital_currency" \o "Moneda digitală) , a creat prima monedă digitală cu eCash.

In 1982 David introduce notiunea de semnaturi digitale. Această formă de semnătură digitală orbește conținutul unui mesaj înainte de a fi semnat, astfel încât semnatarul nu poate determina conținutul. Semnătura oarbă rezultantă poate fi verificată public cu ajutorul mesajului original în modul unei semnături digitale regulate.

În 1989, el (cu Hans van Antwerpen) a introdus [semnături incontestabile](https://en.wikipedia.org/wiki/Undeniable_signature" \o "Semnătura incontestabilă) .  Această formă de semnătură digitală utilizează un proces de verificare care este interactiv, astfel încât semnatarul poate limita cine poate verifica semnătura. Deoarece semnatarii pot refuza să participe la procesul de verificare, semnăturile sunt considerate valabile, cu excepția cazului în care un semnatar folosește în mod specific un protocol de dezacord pentru a demonstra că o semnătură dată nu a fost autentică.

În 1991, el (cu Eugene van Heyst) a introdus [semnături ale grupului](https://en.wikipedia.org/wiki/Group_signature" \o "Semnătura grupului) , care permit unui membru al unui grup să semneze anonim un mesaj în numele întregului grup.  Cu toate acestea, un administrator de grup desemnat deține puterea de a revoca anonimatul oricărui semnatar în cazul litigiilor.

**Comunicare anonimă**

În 1981, Chaum a propus ideea unei rețele anonime de comunicare într-o lucrare.  Propunerea sa, numită [rețele mixte](https://en.wikipedia.org/wiki/Mix_network" \o "Rețea de mixare) , permite unui grup de expeditori să trimită o criptare a unui mesaj și a destinatarului său către un server. Odată ce serverul are un lot de mesaje, acesta va reordona și descărca mesajele astfel încât acest server să știe ce mesaj a venit de la expeditor. Lotul este apoi redirecționat către un alt server care efectuează același proces. În cele din urmă, mesajele ajung la serverul final unde sunt complet decriptate și livrate destinatarului. De asemenea, este propus un mecanism care să permită returnarea mesajelor. Rețelele mixte stau la baza unor [resturi](https://en.wikipedia.org/wiki/Anonymous_remailer" \o "Remiler anonim) și sunt strămoșul conceptual al instrumentelor moderne de navigare web anonime precum [Tor](https://en.wikipedia.org/wiki/Tor_(anonymity_network)) . Chaum a susținut că fiecare router va fi creat, în mod eficient, un nod Tor.

În 1988, Chaum a introdus un tip diferit de sistem de comunicare anonim, numit DC-Net, care este o soluție a problemei propuse pentru [criptograful de mese](https://en.wikipedia.org/wiki/Dining_cryptographers_problem" \o "Problema criptografilor de luat masa) .  DC-Nets este baza instrumentului software Dissent.

### Sisteme de votare de încredere

Chaum a adus numeroase contribuții la securizarea sistemelor de vot, inclusiv prima propunere a unui sistem care poate [fi verificată de la capăt la sfârșit](https://en.wikipedia.org/wiki/End-to-end_auditable_voting_systems) . Această propunere, făcută în 1981, a fost dată ca o aplicație a rețelelor mixte. În acest sistem, voturile individuale ale alegătorilor au fost păstrate private, pe care oricine le-a putut verifica dacă numărul a fost contorizat corect. Aceasta, precum și alte sisteme de vot criptografic timpuriu, au presupus că alegătorii ar putea calcula în mod fiabil valorile cu computerele lor personale. În 1991, Chaum a introdus SureVote, care le-a permis alegătorilor să voteze un sistem de vot de încredere,  propunând un proces numit acum „vot prin cod” și folosit în sistemele de vot la distanță.

În 1994, Chaum a introdus primul sistem de vot în persoană, în care alegătorii au votat electronic la secția de votare și au verificat criptografic că DRE nu și-a modificat votul (sau chiar a aflat despre ce a fost).  În anii următori, Chaum a propus (adesea cu alții) o serie de sisteme de vot verificabile criptografic care utilizează buletine de hârtie convenționale: [Pret a Voter](https://en.wikipedia.org/wiki/Pret_a_Voter" \o "Pretut votant) , [Punchscan](https://en.wikipedia.org/wiki/Punchscan" \o "Punchscan) , și [Scantegritate](https://en.wikipedia.org/wiki/Scantegrity" \o "Scantegrity) . Orașul [Takoma Park, Maryland a](https://en.wikipedia.org/wiki/Takoma_Park,_Maryland) folosit Scantegritatea pentru alegerile din noiembrie 2009.Aceasta a fost prima dată când au fost organizate alegeri din sectorul public folosind orice sistem de vot verificabil criptografic.

***Partea Practica : Semnatura Chaum-van Antwerpen***

Fie *p=*2*q*+1un numar prim cu *q* prim si *α* [apartine]  *Z\*p*,un element de ordin *q.* Pentru 1<= *α<=q*-1 se defineste β= *α*a (*modp*).

*p*=117, *q* = 55=> 55\*2+1.

*α* =7.

Fie G subgrupul de ordin q al lui Z*p* generat de *α.* Se definesc P =A =G, K={*p, α , α ,* β)| β≡ *α* *a*(*mod p*)}. Valorile p, *α,* β sunt publice, iar a este secreta.

*a =29,* β=729(mod117)=76.

Pentru K=(p, *α, α,* β),x ε G se defineste y=*sigk(x)=*x*amodp*.

X=184 cu *y=xamod p.*

*y=xamodp* = 18429 mod 117 = 97.

1. Alice alege aeator numerele *e*1,*e*2 ε Z\**p*: *e*1 = 7, *e*2 = 7.
2. Calculeaza c = ye1 βe2 *mod p* si-l trimite lui Bob.

C=497mod117=49.

1. Bob calculeaza d=c a^(-1) *mod q mod p:*

*d=4929^(-1) mod 55mod 117=*9, si-l trimite lui Alice.

Alice admite autenticitatea lui y daca si numai daca D = xe1\* *αe2mod p.*

*D=* xe1\* *αe2mod p = 14847\*77 mod 117 = 97.*

*Semnatura este valida, deoarece 97=97.*

**Concluzie:**

Dupa executarea aceste llucrari pot afirma a acest algoritm de verificare este interactive astfel: semnatarul participa la verificarea semnaturii. Semnatarul odata ce a generat o semnatura nu poate pretinde ca nu a facut aceasta: ca ex: daca A consta semnatura, poate dovedi ca nu el a generatt aceasta semnatura

Insa-si algoritmul de criptare presupune urmarea a 5 pasi si anume>

**Generarea cheilor.** Genereaa unei cheie publice RSA (n, e) si cheia secreta corespunzatoare d.

**Mascarea mesajului** Alegerea mesajul m ∈ Zn ¸si k ∈ Zn aleatoriu. Calculeaza mesajul mascat m 0 = mke (mod n) pe care il trimite .

**Generarea semnaturii.** Se calculeaza s 0 = (m0 ) d (mod n). Indepartarea mastii. Se calculeaza s = k −1 s 0 (mod n).

**Verificarea semnaturii.** (a) Claire detine ms,(n, e). (b) dac˘a s e = m (mod n) Se accepta semnatura.