There is a diagram with arrows and labels. The text written on the page suggests that it is related to cryptography, with terms like "plaintext (msg)", "ciphertext (c)", "encryption", "decryption", and "key". The diagram appears to illustrate a process involving encryption and decryption, possibly showing the flow of encrypted messages and the use of keys in the encryption and decryption processes.

The handwritten notes indicate a focus on secure communication, encryption, and decryption, with references to terms like "plaintext" and "ciphertext". The diagram likely represents a protocol or a method for secure data exchange, possibly involving concepts like "attack" and "resende attack".
b \rightarrow m \quad E_{pub}(msg) \quad \text{Exposed}
A \cdot B \leq E_{\text{pub}}(E_{\text{priv}}(\text{msg})) \land V_{\text{pub}}(E_{\text{pub}}(\text{msg}))
Dear do the same

After sending next 1/2

Dear do the same

Read Send 1/2 the bold

Write everything inCourier and key

 Internals and more

\[ E_{\text{pub}}(\text{msg}) \rightarrow E_{\text{pub}}(\text{msg}) \rightarrow E_{\text{pub}}(\text{msg}) \]

M \rightarrow A

A \rightarrow E_{\text{pub}}(\text{msg}) \rightarrow M

M \rightarrow E_{\text{pub}}(\text{msg}) \rightarrow A

Feedback?
In cannot continue the scenarios.

Same for B

Sample 12 to A

Sample in null\n
M evidence in mass
$s$ for $c_{\text{ann}}$  

Sym Key  

$\text{Enc}_{\text{pub}(s)}$  

A  

$\text{Enc}_{\text{pub}(s)}$  

$\text{M}_{\text{dec}(s)}$  

$\text{M}_{\text{dec}(s)}$  

High card $c_{\text{ann}}$
\( (s_1, s_2) \) as shown by

Use

\[ (s_1) \quad \text{E.p.m. (S.1)} \quad A \]

B

\[ (s_2) \quad \text{E.p.m. (S.2)} \quad \]

\[ A \]

4
Hash
- match with
  - Alice's pub key
  - Encrypted sig match
    - match with \\
      - take hash of dec
      - verify

If cannot deny

- not irrevocable
- not addressable
- not renewable
- permanent
- L.A. reissues

Digital Signature

A + B = E^p v (A + B)
- Request money from A - B
- Some $ is not crushed yet
- Sign and approve check (2)
- A $25,000 check is needed to be verified
- Be account
- Funds $15,000 key
- You agree check
How A knows B's pub key?
(or vice versa)

Use Digital Certificate

- Bob
- Bob's pub key
- Hash

Sig of Cert Authority (CA)
(Enc hash with private key of CA)
Certificates
- Amazon's private key on web server
- CA's private key
  - on a physically secure computer
Disadvantages of Cellulose System

- Limited supply

- Large area on plane

- Too many cells

- All classes are the same

- No classes of cellulose

- Unknown, but

- Varied and diverse

- Due to the CA de 9 year job of

- Bacterial cellulose production
1. Hash data in cert
2. Same cert verification
3. CA pub key
4. sig decryption with CA pub key = hash
5. sig decrypt with CA

Certificate verification Amazon
Same cert Amazon
Hash data in cert
Get CA pub key
Verify CA sig
Get Amazon pub key
Get Amazon