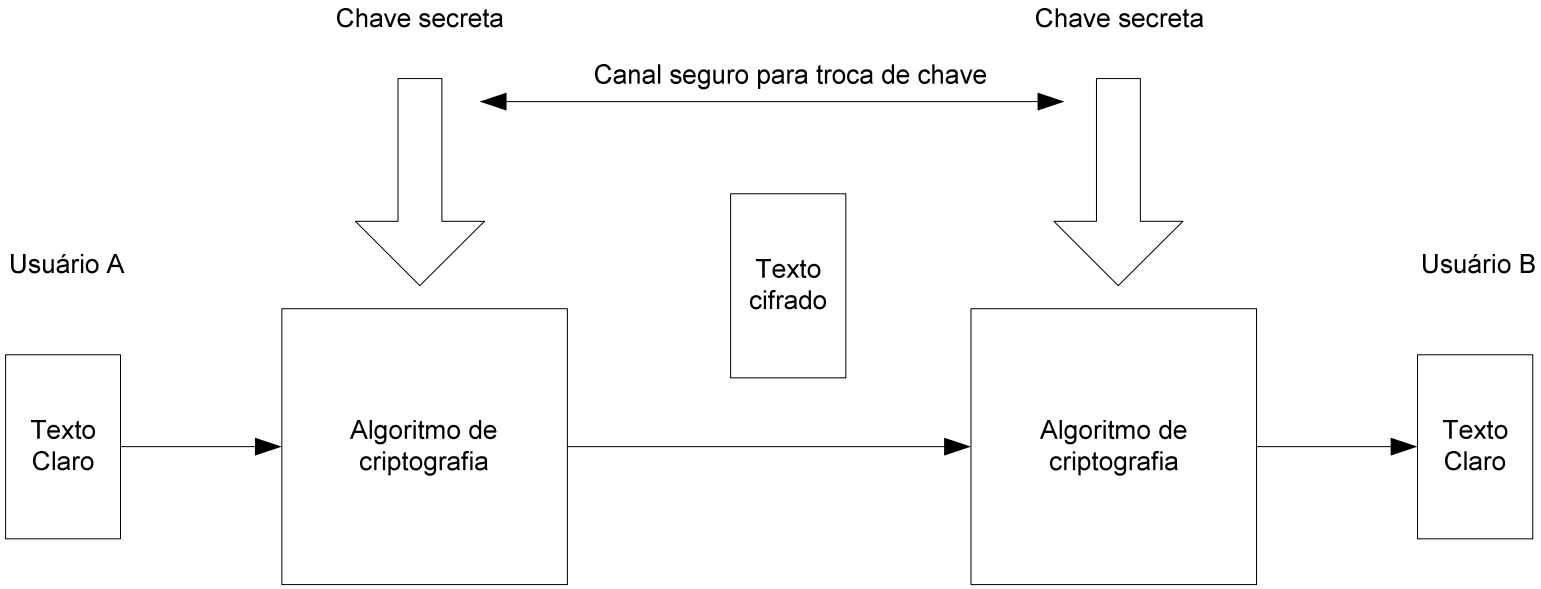
Criptografia Simétrica

- A criptografia simétrica é uma forma de criptossistema em que a criptografia e a decriptografia são realizadas usando a mesma chave. Ela também é conhecida como criptografia convencional ou criptografia de chave única.



Padrões de Criptografia Simétrica

- **Criptografia de Blocos**
  - DES (Data Encryption Standard)

    Tornou-se praticamente inútil em 1998, ao ser quebrado em apenas 3 dias. Alternativas ao DES, sendo as mais importantes AES (Advanced Encryption Standard) e Triple DES.

  - AES (*Advanced Encryption Standard*)

    Trata-se do atual padrão de criptografia dos EUA, utilizados em transações bancárias, redes Wi-Fi e no GPON.

- **Criptografia de Fluxo**
  - RC4 (*Rivest Cipher*)

    Usado para criptografia WEP (*Wired Equivalent Privacy*) e WPA (*Wi-Fi Protected Access*).

Inatel

Instituto Nacional de Telecomunicações

www.inatel.br

Compartilhamento seguro de chaves secretas

- Existem várias formas de distribuir chaves secretas de maneira segura. Normalmente, as formas mais usadas são baseadas no uso da criptografia de chave pública para distribuição das chaves secretas.

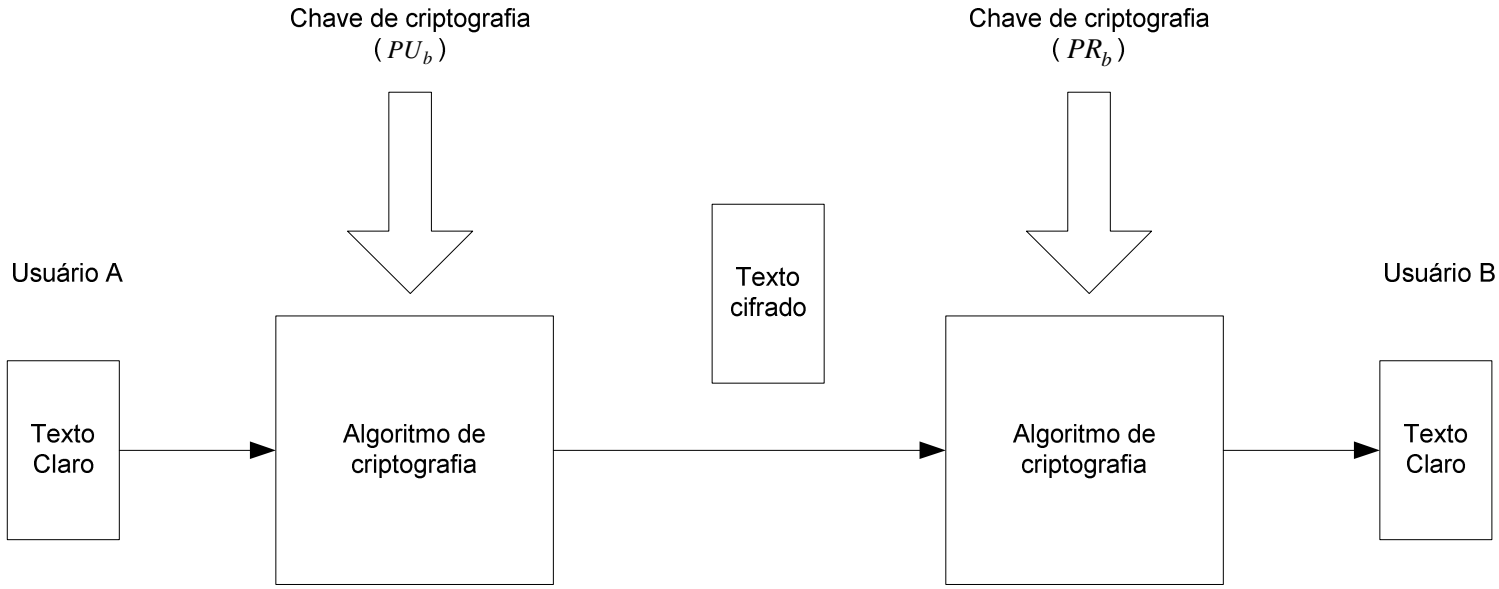
  – Distribuição de chaves secretas com criptografia de chave pública. (Usada no SSL/TLS).

  – Acordo de chaves Diffie-Hellman. (Usada no IP-Sec).

  – Criptografia quântica. (Usada em sistemas QKD (*Quantum Key Distribution*))

Criptografia Assimétrica

- A criptografia assimétrica é uma forma de criptossistema em que a criptografia e a decriptografia são realizadas usando diferentes chaves – uma chave pública (PU_b) e uma chave privada (PR_b). É conhecida também como criptografia de chave pública.



RSA – Rivest Shamir Adlleman

- Publicado em 1978 por 3 professores do MIT é desde então a técnica de uso geral mais aceita e implementada para criptografia de chave pública. Trata-se de um esquema de cifra por bloco.

- Criptografia

$$C = M^{e} \bmod(n)$$

- Decriptografia

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