System Security

Cryptography - Details

Giovanni Russello

Based on Clark’s slides

g.russello@auckland.ac.nz

http://www.cs.auckland.ac.nz/compsci725s2c/

Stream Cipher

- ***P*** $\oplus$ ***S* :** bitstring ***P*** XORed with an arbitrarily-long “keystring” ***S*** generated from our secret key ***K.***
- Decryption is the same function as encryption, because $S \oplus (S \oplus P) = P$
- Very fast and can be built in hardware
- Examples include: A5 (GSM), RC4 (SSL)

Block Ciphers

- Operate on a fixed-length of bit – block
- Based on Product Cipher, a combination of *substitutions* and *permutations*
- Multiple rounds with subkeys derived from the main key
- Examples include:
  - Data Encryption Standard (DES) – block 64-bits, key 56-bits
  - Triple DES – triple encryption of each block with a 168-bits key
  - AES with 128-, 192-, 256-bits key

Iterated Block Ciphers

Iteration of the same transformation (round function) on fixed-size block

$$P_0 = P \oplus K_0$$

$$P_i = R_{Ki}(P_{i-1});\ i=1..n$$

$$C = P_n \oplus K_{n+1}$$

Iterated Block Ciphers

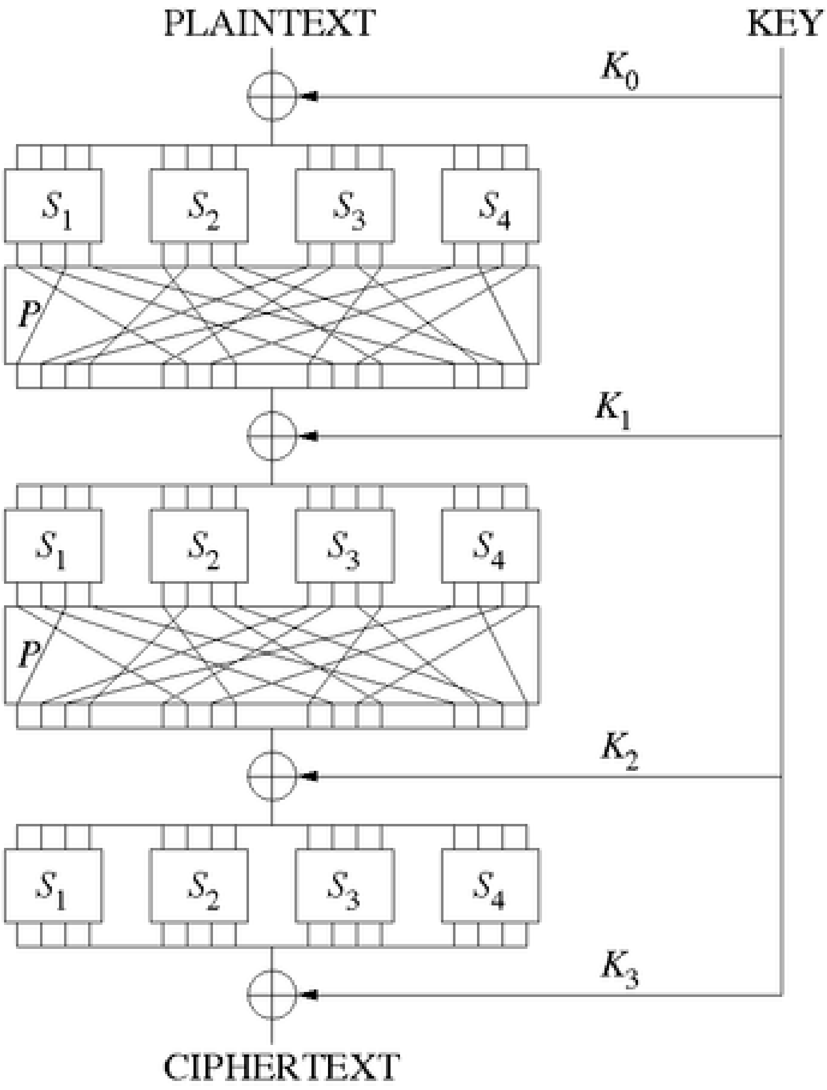


Image source - Wikipedia

Substitution-permutation networks

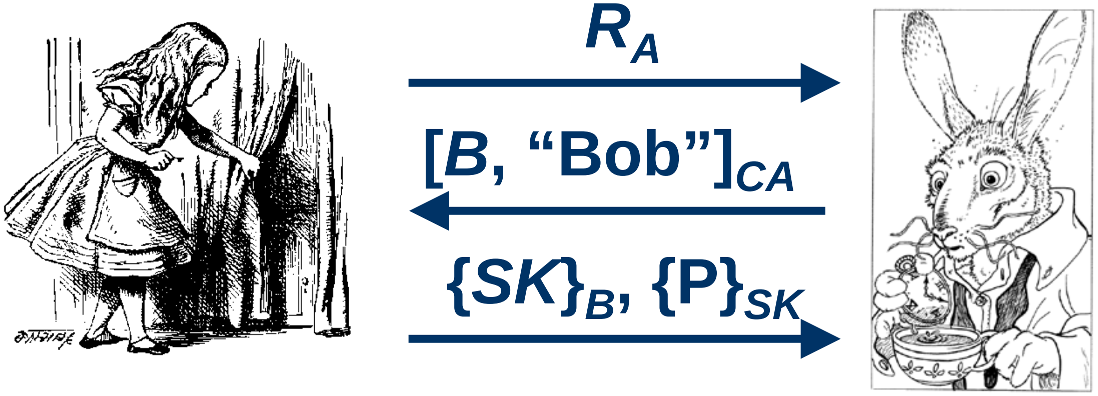
Public Key Cryptography

- Separate keys for encryption (E) and decryption (D): $D(E(P, k_e), k_d) = P$
- The secret key k_e cannot be computed efficiently from the public key k_d and the ciphertext

Authenticating using PK

- Using the secret key we can “sign” a message
  - [“Hello”]$_G$ is a message signed with Giovanni secret key
- Public Key Infrastructure (PKI) to discover public keys
- Certificate Authority (CS) is a registry database

PK Protocol - Naive



R_A

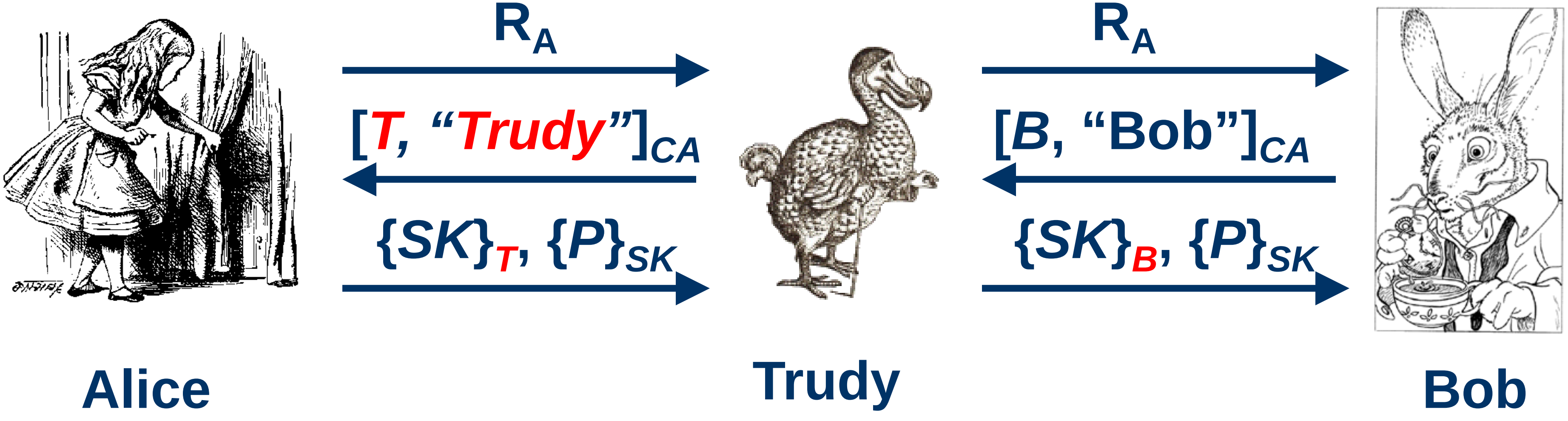
$[B, \text{“Bob”}]_{CA}$

$\{SK\}_B, \{P\}_{SK}$

Alice

Bob

Man in the Middle



R_A

$[T, \text{“Trudy”}]_{CA}$

$\{SK\}_T, \{P\}_{SK}$

R_A

$[B, \text{“Bob”}]_{CA}$

$\{SK\}_B, \{P\}_{SK}$

Alice

Trudy

Bob

Trudy’s certificate might be

$[T, \text{“Bob”}]_{CA’}$

Having a certificate does not means authenticity

Resources

- Security Engineering – Ross Anderson
- Chapter 5: http://www.cl.cam.ac.uk/~rja14/Papers/SEv2-c05.pdf