M2 CyberSecurity
Security Architecture: network, system, key management, cybersecurity of industrial system.

Systems and Network Security

Florent Autréau - florent.autreau@imag.fr
2016 /2017

Network Security - Part 2

- Introduction
- Threat landscape
- Cryptography and Network Security
-

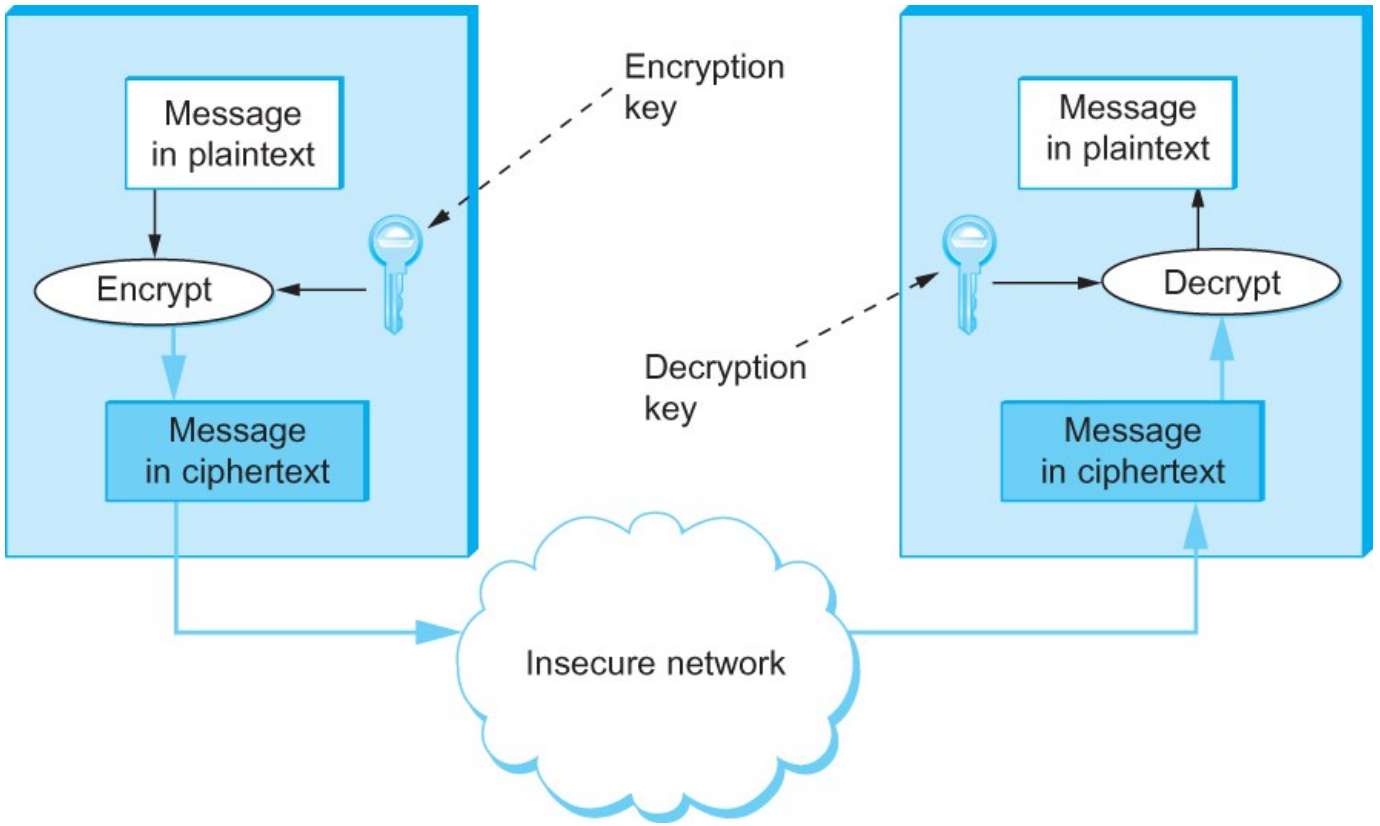
Usages de la Cryptographie

Chiffrement (Encryption): fournit de la confidentialité, ainsi qu'éventuellement de l'authentification et garantit l'intégrité.

Checksums/hash: garantit l'intégrité et peut aussi authentifier.

Signature : authentification, intégrité et irréfutabilité.

Cryptograhic Building Blocks



Symmetric-key encryption and decryption

Types of Ciphers

Stream-based Ciphers

- One at a time, please
- Mixes plaintext with key stream
- Good for real-time services

Block Ciphers

- Amusement Park Ride
- Substitution and transposition

Cryptographic Methods

Symmetric

- Same key for encryption and decryption
- Key distribution problem

Asymmetric

- Mathematically related key pairs for encryption and decryption
- Public and private keys

Cryptographic Methods

Hybrid

Combines strengths of both methods

Asymmetric distributes symmetric key

Also known as a ***session key***

Symmetric provides bulk encryption

Example:

SSL negotiates a hybrid method

Algorithms

Symmetric

DES (Modes: ECB, CBC, CFB, OFB, CM), 3DES, AES, IDEA, Blowfish, Rc4, Rc5, Blowfish

Asymmetric

DH, RSA, El Gamal, ECC

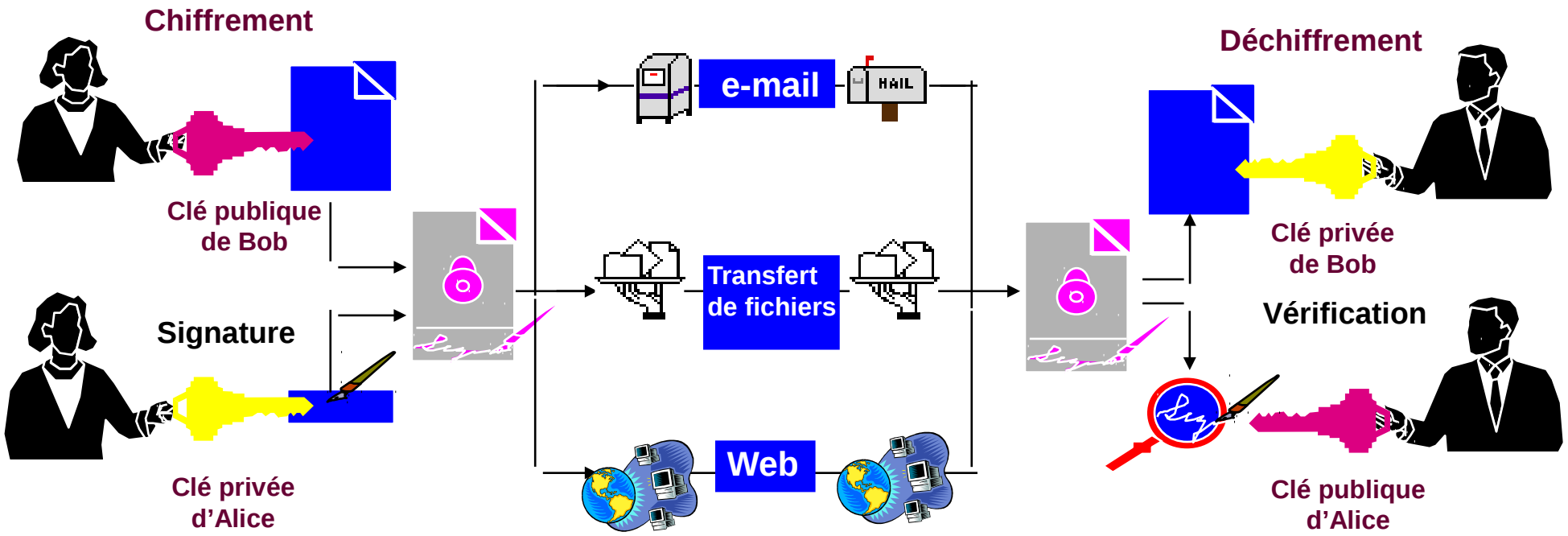
Hashing

MD5, SHA1, SHA-256

Public Key Cryptography Standards - PKCS

- PKCS 7
  - Cryptographic Message Syntax Standard
- PKCS 10
  - Certification Request Syntax Standard - used by Netscape browser, IE, and SSL libraries
- PKCS 11
  - Cryptographic Token Interface Standard - An API for signing and verifying data by a device that holds the key
- PKCS 12
  - Personal Information Exchange Syntax Standard - file format for storing certificate and private key - used to move private information between browsers

Cas d'usages


Chiffrement
Clé publique
de Bob
Signature
Clé privée
d'Alice
e-mail
Transfert
de fichiers
Web
Déchiffrement
Clé privée
de Bob
Vérification
Clé publique
d'Alice

Kerberos

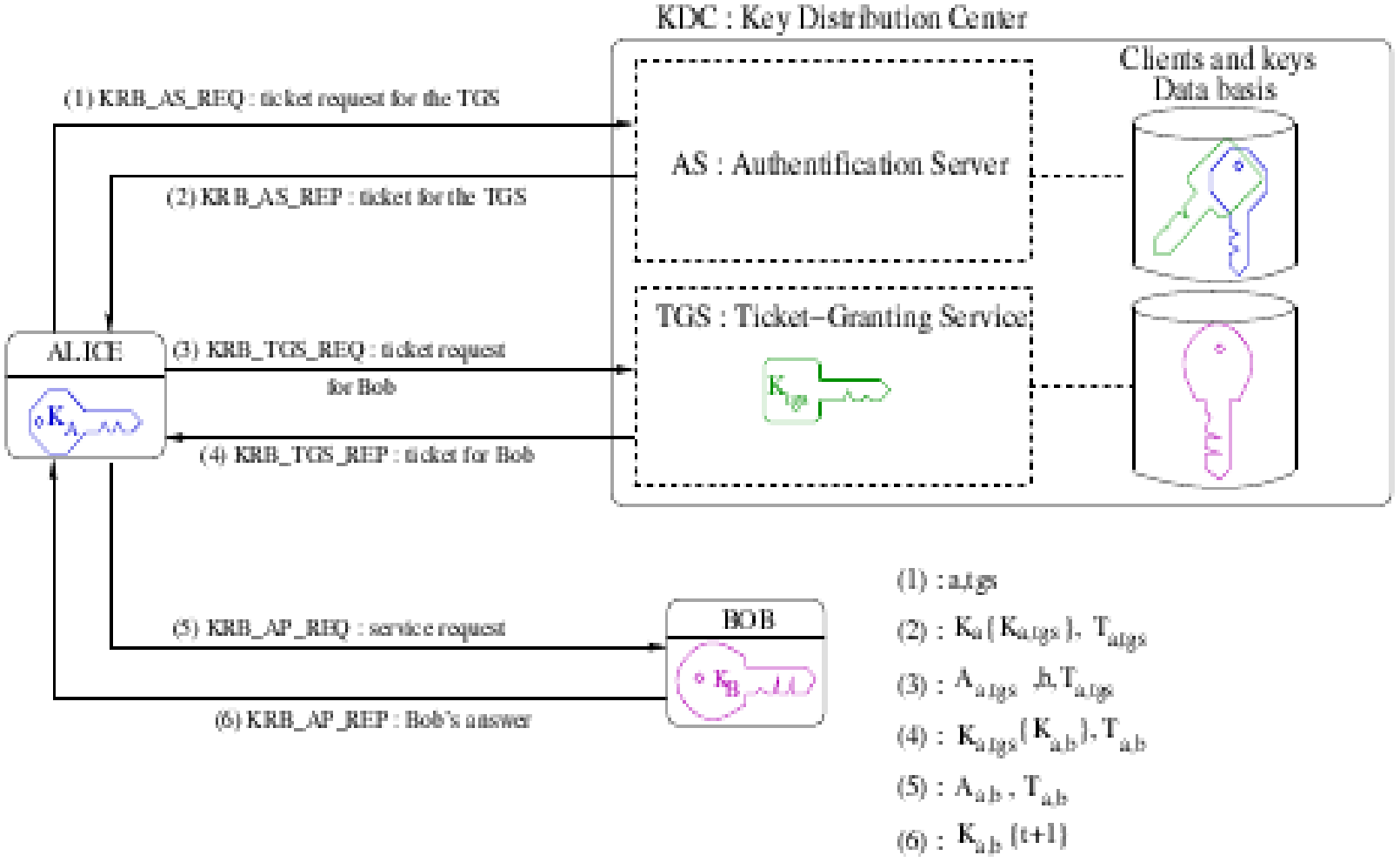


FIG. 1: Les étapes d'authentification Kerberos.

Cryptanalysis

- The study of methods to break cryptosystems
- Often targeted at obtaining a key
- Attacks may be passive or active

Cryptanalysis

- Kerckhoff’s Principle
  - The only secrecy involved with a cryptosystem should be the key
- Cryptosystem Strength
  - How hard is it to determine the secret associated with the system?

Cryptanalysis Attacks

- Brute force
  - Trying all key values in the keyspace
- Frequency Analysis
  - Guess values based on frequency of occurrence
- Dictionary Attack
  - Find plaintext based on common words

Cryptanalysis Attacks

- Replay Attack
  - Repeating previous known values
- Factoring Attacks
  - Find keys through prime factorization
- Ciphertext-Only
- Known Plaintext
  - Format or content of plaintext available

Cryptanalysis Attacks

- Chosen Plaintext
  - Attack can encrypt chosen plaintext
- Chosen Ciphertext
  - Decrypt known ciphertext to discover key
- Differential Power Analysis
  - Side Channel Attack
  - Identify algorithm and key length

Cryptanalysis Attacks

- Social Engineering
  - Humans are the weakest link
- RNG Attack
  - Predict IV used by an algorithm
- Temporary Files
  - May contain plaintext