Introduction to Cryptography

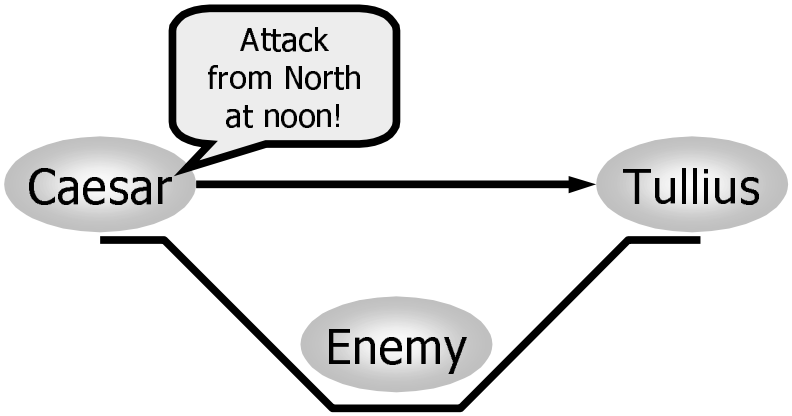
CSCI-7000-001 fall'01

Antonio Carzaniga

Outline

- What is cryptography about?
- What is cryptanalisis about?
- Cryptography in context: cost vs. time
- Main classes of cryptographic functions
- Most important algorithms

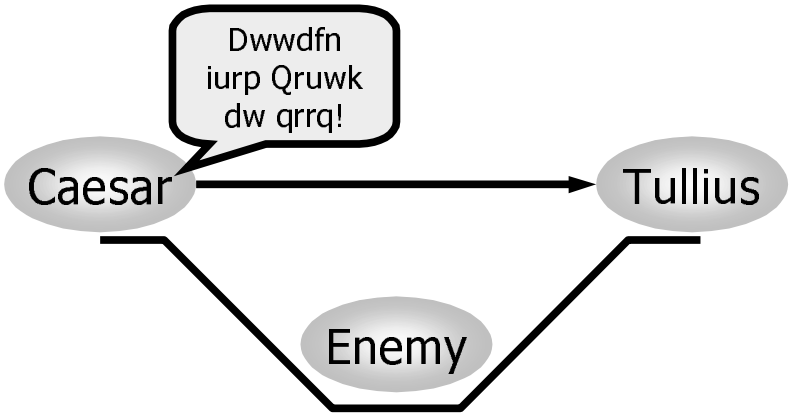
Example



Example

- Caesar and his general Tullius on opposite side of the enemy post
- Caesar wants to send his general Tullius an order to attack coming from the North at noon
- …but he doesn't want the enemy to know that
- Also Tullius wants to make sure that the order is authentic

Caesar Cipher



Caesar Cipher

- *Shift* every letter by 3 positions in alphabet
  - A → D
  - B → E
  - …
  - Y → B
  - Z → C

Breaking Caesar Cipher

- Enemy might expect the first word to be "Attack"

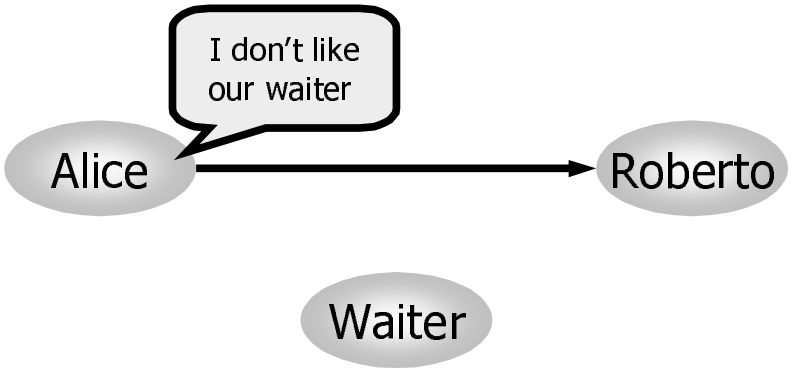
A	T	T	A	C	K
D	W	W	D	F	N

- Observations
  - Ciphertext is same length as plaintext
  - Same letters in plaintext correspond to same letters in ciphertext
  - ...

Cryptanalisis

- Attacks to encryption schemas
  - ciphertext attack
  - known plaintext attack
  - chosen plaintext attack
- Methods
  - statistical distributions of words
  - other structural aspects of plaintext
  - ...

Example (2)



Example (2)

- Alice and Roberto at a restaurant in Boulder
- Alice wants to tell Roberto that she doesn't like their waiter
- but doesn't want the waiter to know that
- ...so they could speak Italian
- but the waiter might suspect that they're saying something bad

Steganography

- Hiding messages within plaintext messages
- a.k.a. *watermarking*

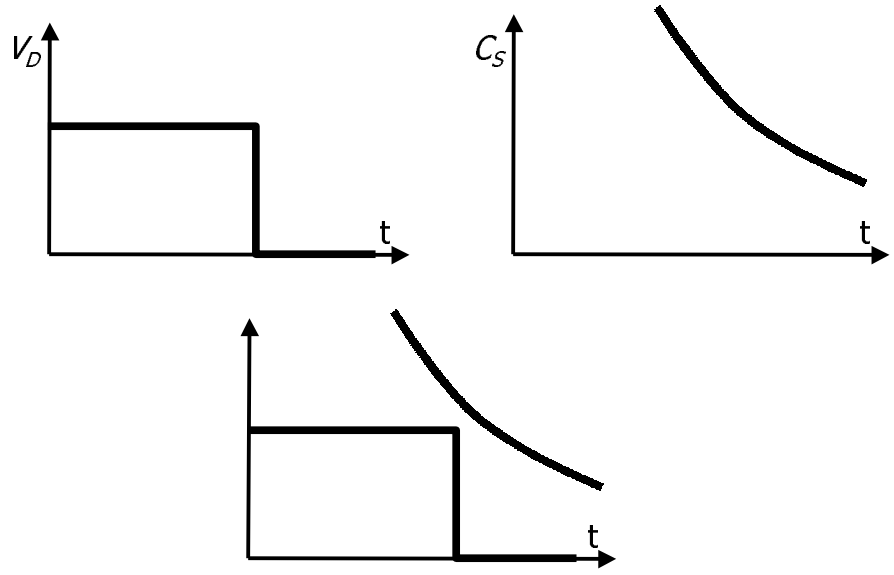
Cryptography in Context

- Prevention (protection) methods
  - for confidentiality
- Detection methods
  - for integrity
  - for authentication

Value of Cryptographic Protection

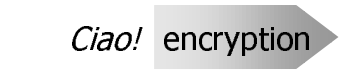
- Breaking an encryption scheme is a matter of
  - time
  - (to some extent) money, to buy large computers
- Necessary assessment
  - value function for information *D*
    $value_D = V_D(t)$
  - cost of breaking schema *S*
    $cost_S = C_S(t)$: cost of breaking *S* within *t*

Value of Cryptographic Protection



Cryptographic Functions

$y = \mathbf{f}(x)$

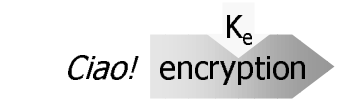


*ciphertext=**E**(plaintext)*

*plaintext=**D**(ciphertext)*

- $\mathbf{D} \equiv \mathbf{E}^{-1}$, *i.e., plaintext=**D**(**E**(plaintext))*
- a.k.a. *restricted algorithms*

Algorithms with Keys



*ciphertext=**E**$_K$(plaintext)*

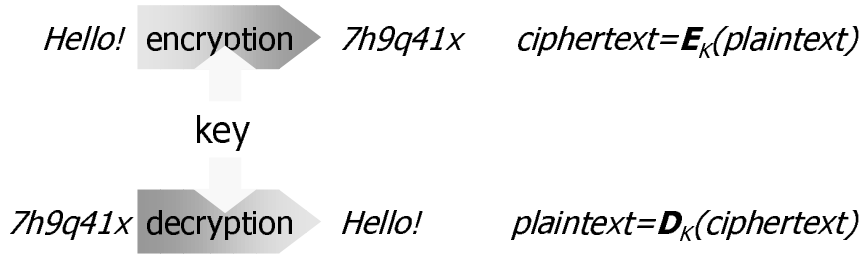
*plaintext=**D**$_K$(ciphertext)*

In practice: $\mathbf{K}_e = \mathbf{K}_d$

Types of Cryptographic Functions

- Secret Key cryptography
  - one key
- Public Key cryptography
  - two keys
- Hash functions
  - no keys

Secret Key Cryptography

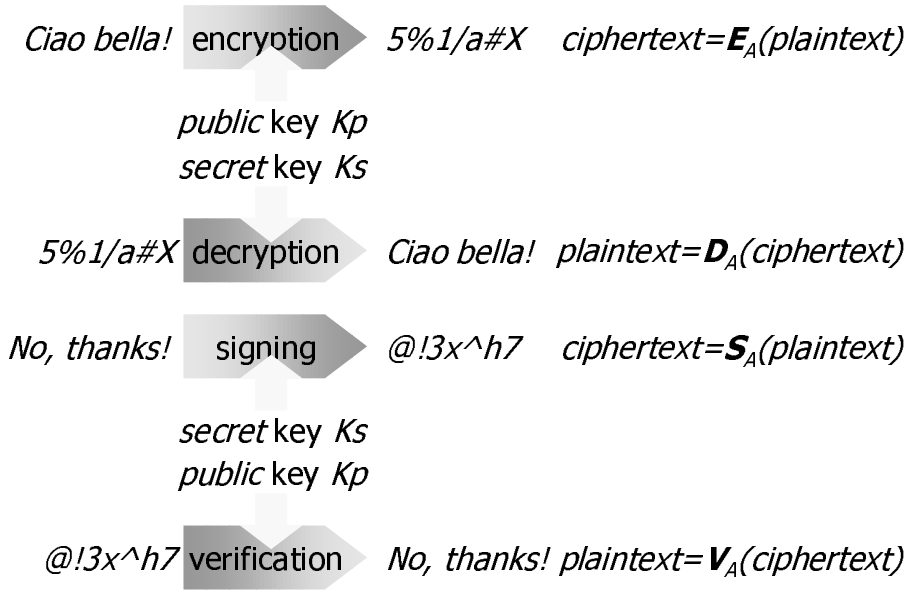


- $K_e \equiv K_d \equiv K$
- $D_K \equiv E_K^{-1}$, i.e., $plaintext = D_K(E_K(plaintext))$
- a.k.a. *conventional* or *symmetric* cryptography

Public Key Cryptography

- Invented by W. Diffie and M. Hellman (1976)
  - although NSA had claimed knowledge since 1966
- Two keys
  - *secret* key (or private key) *Ks*
  - *public* key *Kp*
  - it's intractable to compute *Ks* from *Kp*

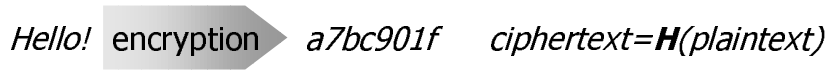
Public Key Cryptography



Public Key Cryptography

- Encryption: ***E*** encryption with *Kp*
- Decryption: ***D*** decryption with *Ks*
- Signing: ***S*** encryption with *Ks*
- Verification: ***V*** decryption with *Kp*
- $\boldsymbol{D}=\boldsymbol{E}^{-1}$, i.e., *plaintext*=$\boldsymbol{D}$(*plaintext*))
- $\boldsymbol{V}=\boldsymbol{S}^{-1}$, i.e., *plaintext*=$\boldsymbol{V}$(*plaintext*))
- a.k.a. *asymmetric* cryptography

Hash Functions



- $\boldsymbol{H}^{-1}$ is not tractable
- |*ciphertext*| = 100~1000 bit
- randomness: any two output ciphertext should be completely uncorrelated, no matter how similar the inputs are
- a.k.a. *one way* functions

Protocols

- Every party knows every step of the protocol in advance
- Every party must agree to follow the protocol
- A protocol must be unambiguous
- A protocol must be complete

Cryptographic Protocols

- Authentication
- Key exchange
- Authentication and key exchange
- Secret splitting and sharing
- Undeniable digital signatures
- Certification
- Subliminal channel
- Proxy signature
- Group signature

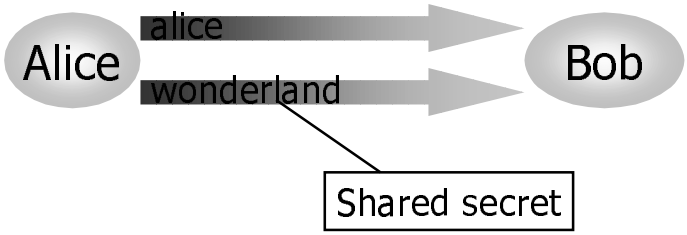
More Cryptographic Protocols

- Computing on encrypted data
- Prediction commitment
- Fair coin flip
- Mental poker
- Key escrow
- Zero-knowledge proof
- Simultaneous contract signing
- Digital certified mail
- Simultaneous exchange of secrets

Esoteric Protocols

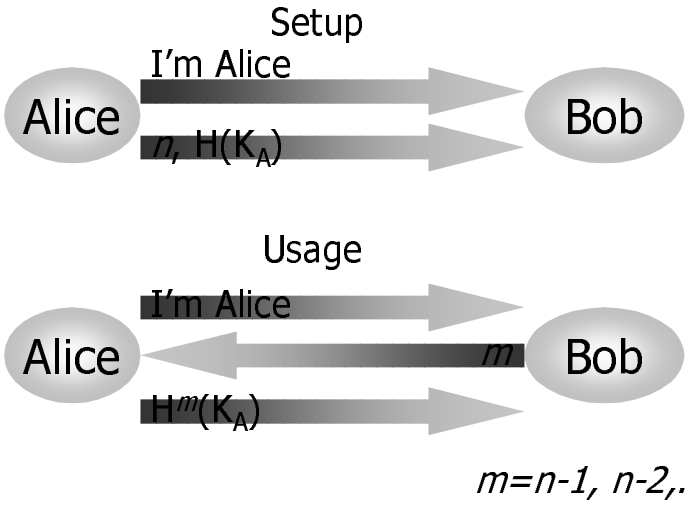
- Secure elections
- Secure multiparty computations
- Anonymous message broadcast
- Digital cash (or anonymous digital cash)

Plaintext Authentication



- Alice sends her secret password
- Bob verifies that the password is correct
- Bob does not need to store the password, it can store a hash of the password
- Vulnerable to eavesdropping

Hash Function Authentication



Analysis of SKey

- Vulnerabilities?

  ...