Introduction to Cryptography

M. Prem Laxman Das

March 18, 2025

Society for Electronic Transactions and Security

Table of contents

Cryptography in Epigraphy

Language, Writing System and Decipherment

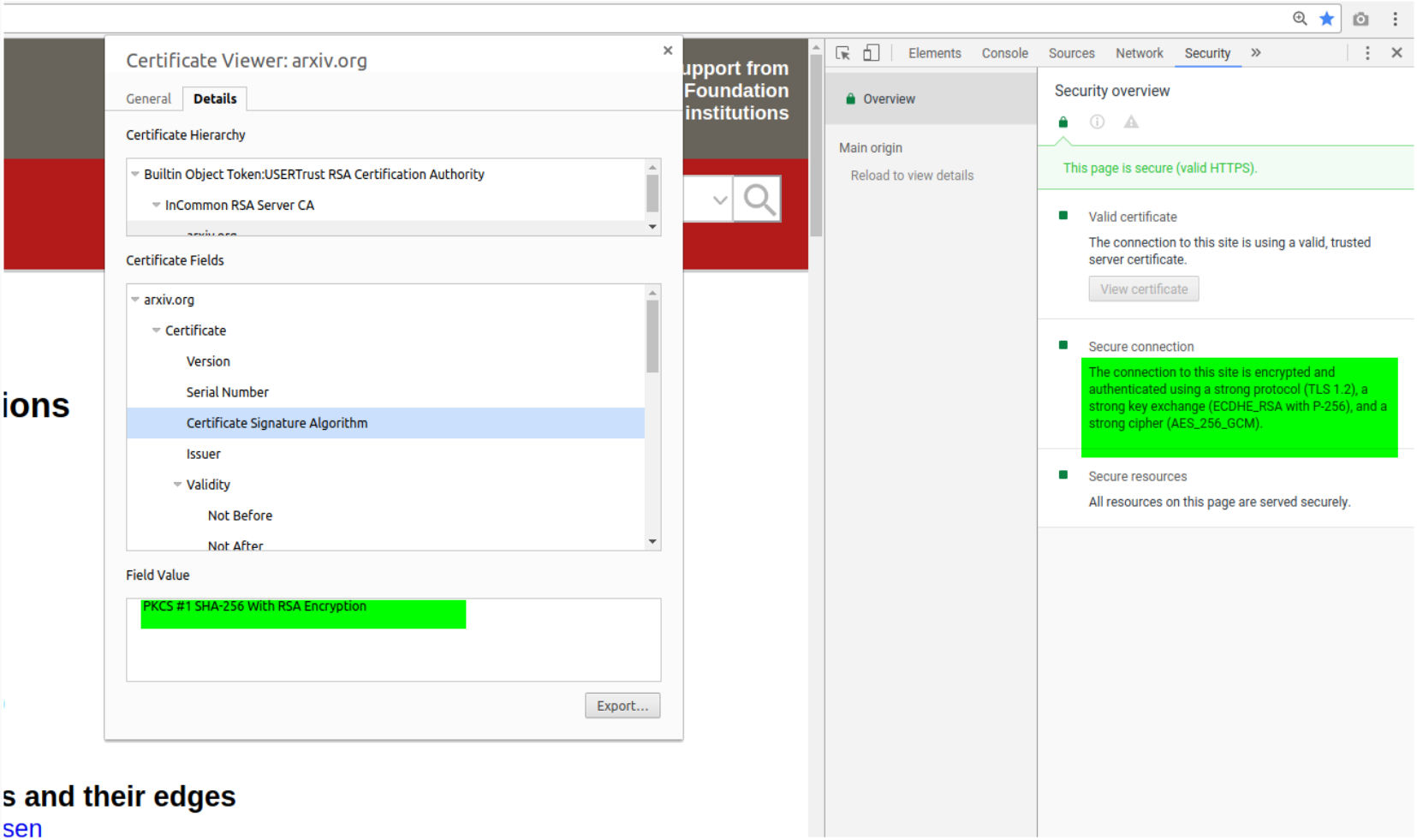
- A writing system is a notational system for a language, various categories based on phonetics and semantics
- Decipherment refers to the process of determination of the symbol system behind the unknown script or text
- Four types of decipherments based on known / unknown language and writing system
- Many challenges: reading direction, unknown punctuation, small dataset, incomplete vocabulary, etc

Epigraph Decipherment

- Review of historical alphabets
- Statistical analysis on single characters
- Statistical analysis of N-grams
- "Encrypted epigraphy - the case of a mysterious inscription in the Neapolitan church of Santa Maria La Nova" by Cosimo Palma

Introduction

TLS Security



What is Cryptology

♣Cryptology is the study and practice of techniques for secure communications in the presence of adversary.

♣It is derived from Greek words "*kryptos*" meaning hidden or secret and "*logia*" meaning study

♣Cryptology comprises of:

- Cryptography – Design of secure systems
- Cryptanalysis – Analyzing or breaking such systems

♣Is very ancient and has found mention in various scriptures.

♣Very important in defence, banking, governance, etc.

Kerckhoffs Principle

♣In 1883 Auguste Kerckhoffs wrote two journal articles on La Cryptographie Militaire, in which he stated six design principles laid down for military ciphers.

♣In modern cryptologic parlance, it is stated as: A cryptosystem should be secure even if everything about the system, except the key, is public knowledge.

♣The same was stated by Claude Shannon as follows: The enemy knows the system.

Goals of Cryptology

Using cryptology, we hope to achieve

Confidentiality – No third party can read the message

Authentication – The sender knows that the receiver knows a particular private key

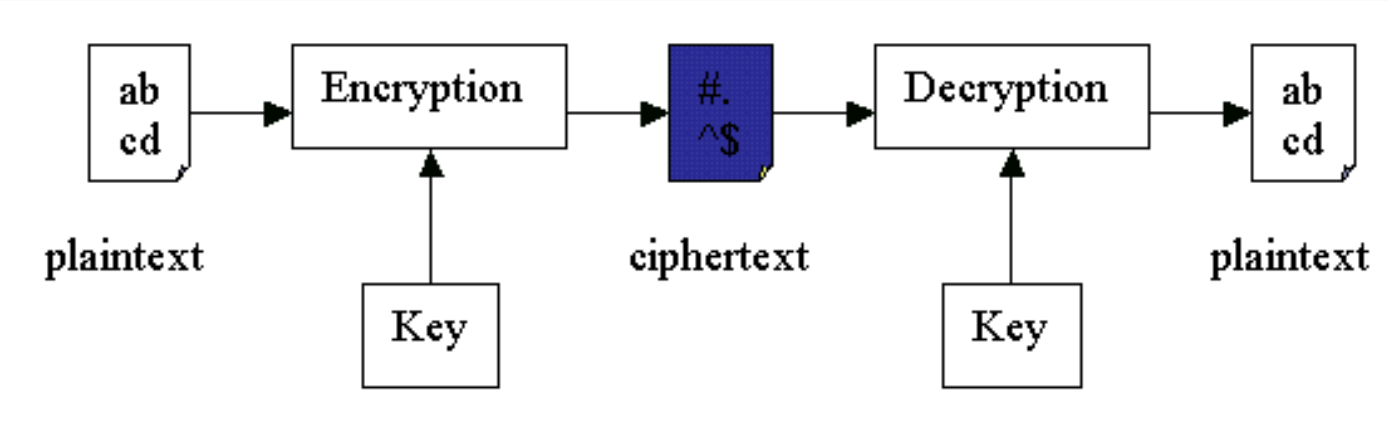
Identification – Binding between the private key and the individual

Trust – Third party certifies that a particular private key belongs to a particular individual

Integrity – Messages are not corrupted during transit

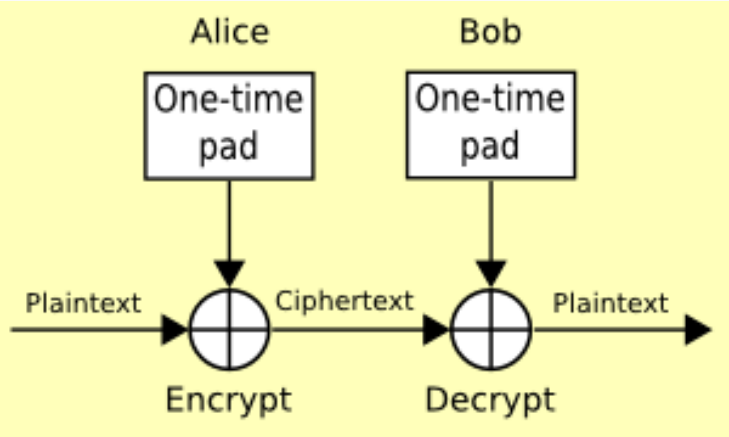
Cryptology Model

♣Sender encrypts message using a key and sends through a public channel, which the receiver decrypts



♣The encryption and the decryption keys may not be the same

One-time Pad



♣Provides perfect secrecy: Knowledge of the ciphertext has no bearing on the plaintext

♣Does not ensure authentication

♣But impractical since

- We need synchronized truly random bits
- Key stream bits cannot be re-used

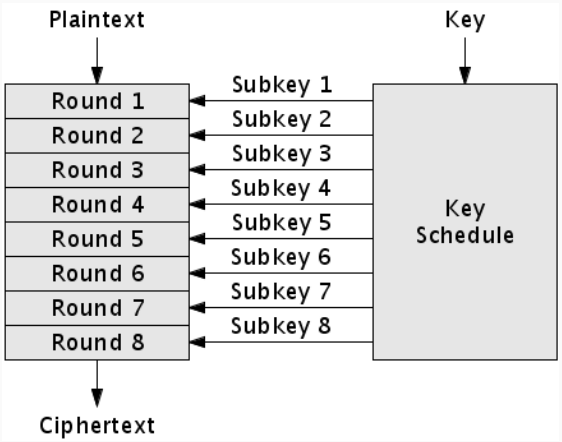
Symmetric Key Cryptography

Symmetric Key Encryption

- Here the encryption and the decryption keys are essentially the same
- Such algorithms assume that the two parties have the same key
- Two broad class of primitives which provide data confidentiality
  1. Stream Ciphers
  2. Block Ciphers
- Hash Functions are used to provide integrity and authentication

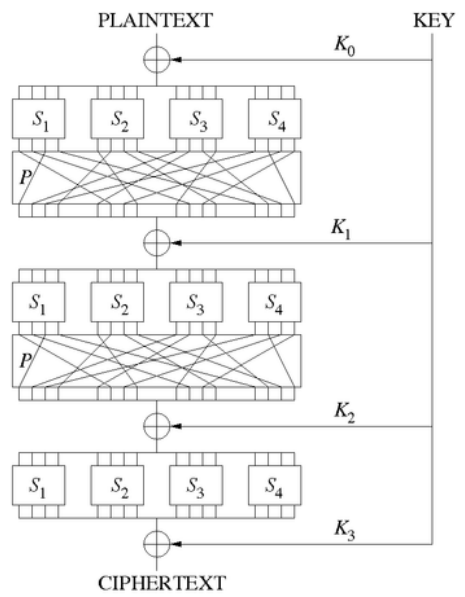
Block Cipher

- Encrypts blocks of message bits
- Usually a iterated cipher
- KSA provides the round keys



- Two broad types

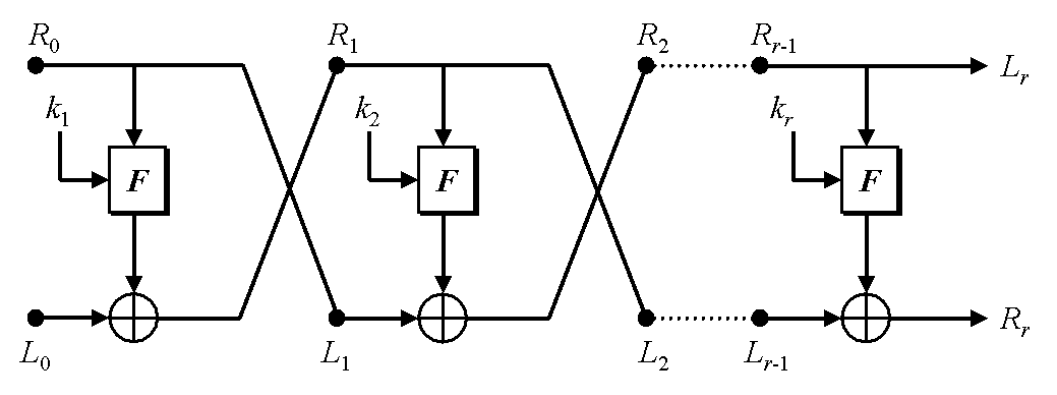
SPN



♣S-boxes for providing non-linearity and linear layer for diffusion of bits. Also key dependence is present.

♣AES: Advanced Encryption Standard

Feistel



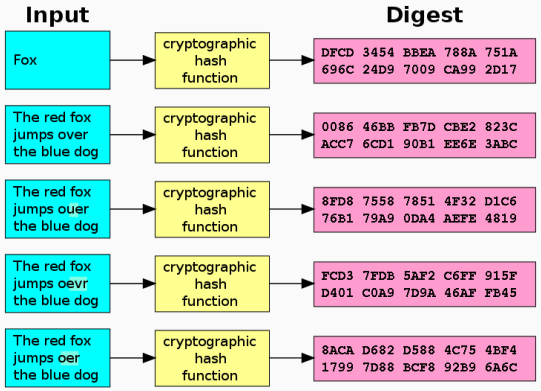
- Left and right parts
- Non-linear function which is key dependent
- DES: Data Encryption Standard

Stream Cipher

- Encrypts message bits by XOR-ing with pseudorandom bits
- Pseudorandom bits are generated using shift registers
- Notice similarity with OTP
- Examples:Salsa and SNOW
- Two types of stream ciphers

1. Synchronous – The pseudorandom bits are generated independently of plaintext and ciphertext bits
2. Self-synchronizing – The pseudorandom bits are dependent on plaintext and ciphertext bits

Hash Functions



♣SHA family: Secure Hash Algorithm

♣Must have the following properties:

1. Pre-image resistance
2. Second pre-image resistance
3. Collision resistance

CBC-MAC

1. One of the more popular ways to construct a MAC is to use a block cipher in CBC mode with a fixed (public) initialization vector
2. In CBC mode, each ciphertext block y_i is XOR-ed with the next plaintext block, x_{i+1}, before being encrypted with the secret key K
3. Let $y_0 = IV$. Construct subsequent ciphertext blocks
$$y_i = e_K(y_{i-1} \oplus x_i)$$
4. Basically, we "encrypt" the plaintext in CBC mode and we only retain the last ciphertext block, which we define to be the tag

Important Attack Models: Encryption

1. Ciphertext only:attacker, with access only to ciphertexts, has to find one of the messages and / or the key
2. Known plaintexts: attacker is given many plaintext - ciphertext pairs and has to find the plaintext for a new ciphertext
3. Chosen plaintexts: Attacker chooses plaintexts and gets the corresponding ciphertexts; the attacker has to find the key or the plaintext corresponding to a new ciphertext

Public Key Cryptography

Limitations of Symmetric Key Systems

♣ Key Distribution: Storage and management of large number of secret keys

♣A Key Distribution Centre can be used, but inapplicable in the case of open systems

♣Attack on the KDC breaks the system

♣If KDC breaks down secure communication is not possible

♣Use public key systems to overcome these shortcomings

Cyclic Groups

♣Let $G = \{1 = g^0, g^1, \ldots, g^{l-1}\}$. This satisfies $g^l = 1$. There is an underlying composition.

♣Example: $\{0, 1, 2, \ldots, m-1\}$ under addition modulo m.

♣Example: $\{1, 2, \ldots, p-1\}$ under multiplication modulo p. The set of non-zero elements of a finite field forms a cyclic group under multiplication.

♣**Discrete Log:** Given g and $h = g^\ell$, find that ℓ. We want such structures where this problem is computationally hard.

♣**Diffie Hellman:** Given $g, h_1 = g^a, h_2 = g^b$ computing g^{ab} is hard.

Diffie-Hellman Key Exchange

DH Key Exchange

Input: Security parameter 1^n

- Alice runs the setup algorithm $\mathcal{G}(1^n)$ to obtain G, q, g
- Alice uniformly chooses $x \in_R \mathbb{Z}_q$ and computes $h_A = g^x$
- Alice sends (G, q, g, h_A) to Bob
- Bob receives the tuple and parses it. He uniformly chooses $y \in_R \mathbb{Z}_q$ and computes $h_B = g^y$. Bob sends h_B to Alice and computes $k_B = h_A^y$
- Alice receives h_B and computes $k_A = h_B^x$

Verify that $k_A = h_B^x = (g^y)^x = (g^x)^y = h_A^y = k_B$

ElGamal Public Key Encryption

Setup. Let $\mathcal{F}_p^* = \langle \alpha \rangle$. Then a is chosen at random and set $\beta = (\alpha)^a \pmod{p}$. Set $P = (p, \alpha, \beta)$ and $S = a$.

Encrypt(x). Choose k at random. Set

$$e(x, P) = y = (\alpha^k \pmod{p}, x\beta^k \pmod{p})$$

Decrypt(y). For $y = (y_1, y_2)$, define

$$d(y, S) = y_2(y_1^a)^{-1} \pmod{p}$$

Under the assumption that discrete log problem is hard, it is infeasible to break the ElGamal cryptosystem.

Authentication: Motivation for Using Digital Sigantures

♣ Plays a very vital role in a PKI

♣ Software updates, such that

- any client can verify that the update is authentic
- no malicious third party can fool a client into accepting a spurious update

♣ To achieve this, the company can do the following:

Software Authentication

- Generate a public key-secret key pair and distribute its public key to every client (bundles with the original software)
- When releasing an update m, the company can compute a signature σ using its secret key and send (m, σ) to every client. The client verifies that σ is a genuine signature on m using the company's public key. Accepts the update when the signature is genuine.

Definition

A digital signature scheme $\mathcal{S}$ consists of three poly-time algorithms $(Gen, Sign, Vrfy)$ such that:

1. The key generation Gen is a PPT algorithm which takes as input the security parameter 1^n and outputs the public key-secret key pair (pk, sk) of length n.
2. The signing $Sign$ is a PPT algorithm which computes $\sigma = Sign(sk, m)$.
3. The verification $Vrfy$ is a deterministic algorithm which outputs a bit $b = Vrfy(Pk, m, \sigma)$.

It is required that, for every legal message $b = 1$ holds.

If there exists a function ℓ such that the message space is $\{0,1\}^{\ell(n)}$ for every output of Gen, then $\mathcal{S}$ is said to be a signature scheme for messages of length $\ell(n)$.

Thank You