

# La Carte à Microprocesseur

## Un système embarqué en plein essor

**Tegawendé F. Bissyandé**  
tegawende.bissyande@fasolabs.org

*Cours préparé pour*  
L'Institut Supérieur de Technologie (IST Burkina)

24 Février 2015

# Rappels chapitres précédents...

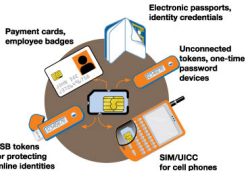


## WHAT IS SMART CARD TECHNOLOGY?



Smart card technology uses a little computer and software with 100s of built-in security features...

... to create personal, portable security devices...



Copyright Gemalto

Marketing de base... Gemalto

## Serious Online Security

How **smart cards** provide solutions to software-based security problems

### PROBLEMS WITH SOFTWARE-BASED SECURITY APPLICATIONS

Single sign-on, password vaults and other software-based security applications consolidate multiple passwords, but leave them vulnerable.

1 If passwords are the only protection used, then anyone obtaining the password can gain access to the system.



2 A master password is vulnerable to...



And a master password is static: once stolen, it can be used anytime.

3 Insiders and IT contractors can compromise master password files.



### SOLUTIONS PROVIDED BY SMART CARDS



A smart card is a small computer that is separate from the desktop, and is used as part of the authentication process.

1 You must physically have the smart card or token for network or information access.



2 A smart card is invulnerable to keyboard logging because security key calculations are done by the computer inside it; only encrypted information passes through the computer.



\* Every authentication is unique and created on the fly.

3 Since insiders cannot log in without the tokens, and there is no master password, smart cards are virtually impossible to attack. Smart card technology is already at the heart of security systems for billions of dollars of individual transactions worldwide in mobilecom, banking, cable and satellite TV, and the U.S. Department of Defense.



# La sécurité dans la carte à puce

## A quels niveaux ?

- physique (*besoin de matériel d'accès aux données*)
- du modèle de système de fichier (*condition d'accès*)
- de la carte (*identification mutuelle entre la carte et l'application qui l'utilise*)
- au niveau des fichiers (*Mot de passe ou code PIN pour accéder à un fichier*)



## Garder en mémoire...

- Sécurité de la carte à puce : ensembles de moyens très efficaces
- Application mal implémentée  $\Rightarrow$  carte défaillante

# Quelques commandes relatives à la sécurité

## VERIFY

- Vérifier un password - comparaison avec info stockée
- "Mot de passe" transite en clair
- Nombre d'échecs comptés (e.g., code PIN de SIM)

## INTERNAL AUTHENTICATE

- Authentifier la carte vis-à-vis du lecteur
- Utilisation de fonctions cryptographiques
- A/R d'infos entre la carte et le lecteur

## GET CHALLENGE

- Utilisé en conjonction avec EXTERNAL AUTHENTICATE
- Demande à la carte la génération d'un *challenge*

## EXTERNAL AUTHENTICATE

- Authentifier l'app du lecteur vis-à-vis de la carte
- Le pendant de INTERNAL AUTHENTICATE

## ENVELOPE

- Envoi d'une commande à l'intérieur d'une commande
- Possibilité de crypter entièrement les data dans l'APDU de la commande
- Utilisée pour se prémunir contre l'espionnage des communications lecteurs $\longleftrightarrow$ cartes

# Quelques commandes relatives à la sécurité

## VERIFY

- Vérifier un password - comparaison avec info stockée
- "Mot de passe" transite en clair
- Nombre d'échecs comptés (e.g., code PIN de SIM)

## INTERNAL AUTHENTICATE

- Authentifier la carte vis-à-vis du lecteur
- Utilisation de fonctions cryptographiques
- A/R d'infos entre la carte et le lecteur

## GET CHALLENGE

- Utilisé en conjonction avec EXTERNAL AUTHENTICATE
- Demande à la carte la génération d'un *challenge*

## EXTERNAL AUTHENTICATE

- Authentifier l'app du lecteur vis-à-vis de la carte
- Le pendant de INTERNAL AUTHENTICATE

## ENVELOPE

- Envoi d'une commande à l'intérieur d'une commande
- Possibilité de crypter entièrement les data dans l'APDU de la commande
- Utilisée pour se prémunir contre l'espionnage des communications lecteurs $\longleftrightarrow$ cartes

# Quelques commandes relatives à la sécurité

## VERIFY

- Vérifier un password - comparaison avec info stockée
- "Mot de passe" transite en clair
- Nombre d'échecs comptés (e.g., code PIN de SIM)

## INTERNAL AUTHENTICATE

- Authentifier la carte vis-à-vis du lecteur
- Utilisation de fonctions cryptographiques
- A/R d'infos entre la carte et le lecteur

## GET CHALLENGE

- Utilisé en conjonction avec EXTERNAL AUTHENTICATE
- Demande à la carte la génération d'un *challenge*

## EXTERNAL AUTHENTICATE

- Authentifier l'app du lecteur vis-à-vis de la carte
- Le pendant de INTERNAL AUTHENTICATE

## ENVELOPE

- Envoi d'une commande à l'intérieur d'une commande
- Possibilité de crypter entièrement les data dans l'APDU de la commande
- Utilisée pour se prémunir contre l'espionnage des communications lecteurs←→cartes

# Quelques commandes relatives à la sécurité

## VERIFY

- Vérifier un password - comparaison avec info stockée
- "Mot de passe" transite en clair
- Nombre d'échecs comptés (e.g., code PIN de SIM)

## INTERNAL AUTHENTICATE

- Authentifier la carte vis-à-vis du lecteur
- Utilisation de fonctions cryptographiques
- A/R d'infos entre la carte et le lecteur

## GET CHALLENGE

- Utilisé en conjonction avec EXTERNAL AUTHENTICATE
- Demande à la carte la génération d'un *challenge*

## EXTERNAL AUTHENTICATE

- Authentifier l'app du lecteur vis-à-vis de la carte
- Le pendant de INTERNAL AUTHENTICATE

## ENVELOPE

- Envoi d'une commande à l'intérieur d'une commande
- Possibilité de crypter entièrement les data dans l'APDU de la commande
- Utilisée pour se prémunir contre l'espionnage des communications lecteurs←→cartes

# Quelques commandes relatives à la sécurité

## VERIFY

- Vérifier un password - comparaison avec info stockée
- "Mot de passe" transite en clair
- Nombre d'échecs comptés (e.g., code PIN de SIM)

## INTERNAL AUTHENTICATE

- Authentifier la carte vis-à-vis du lecteur
- Utilisation de fonctions cryptographiques
- A/R d'infos entre la carte et le lecteur

## GET CHALLENGE

- Utilisé en conjonction avec EXTERNAL AUTHENTICATE
- Demande à la carte la génération d'un *challenge*

## EXTERNAL AUTHENTICATE

- Authentifier l'app du lecteur vis-à-vis de la carte
- Le pendant de INTERNAL AUTHENTICATE

## ENVELOPE

- Envoi d'une commande à l'intérieur d'une commande
- Possibilité de crypter entièrement les data dans l'APDU de la commande
- Utilisée pour se prémunir contre l'espionnage des communications lecteurs←→cartes



# Notions de cryptographie

## Vocabulaire:

- **Texte en clair** : Données compréhensibles qu'un expéditeur veut envoyer à un destinataire
- **Texte Chiffré / Cryptogramme** : Données incompréhensibles obtenu à partir du texte en claire
- **Chiffrement** : Processus transformant le texte en clair en texte chiffré
- **Déchiffrement/Décryptage** : Processus inverse du chiffrement
- **Cryptographie** : science consistant à garder les messages secrets
- **Cryptographe** : Individu pratiquant de la cryptographie
- **Cryptanalyste** : Individu spécialisé dans le décryptage des messages chiffrés  
⇒ ennemi du cryptographe
- **Cryptologie** : Branche mathématique s'intéressant au cryptage
- **Chiffrement continu / par blocs** : selon que les données à crypter sont découpées en blocs ou pas

## Equations

- 1  $C = E(M) \leftarrow$  chiffrement
- 2  $D(C) = M \leftarrow$  déchiffrement
- 3  $D(E(M)) = M \leftarrow$  Equivalence

# Notions de cryptographie

## Vocabulaire:

- **Texte en clair** : Données compréhensibles qu'un expéditeur veut envoyer à un destinataire
- **Texte Chiffré / Cryptogramme** : Données incompréhensibles obtenu à partir du texte en claire
- **Chiffrement** : Processus transformant le texte en clair en texte chiffré
- **Déchiffrement/Décryptage** : Processus inverse du chiffrement
- **Cryptographie** : science consistant à garder les messages secrets
- **Cryptographe** : Individu pratiquant de la cryptographie
- **Cryptanalyste** : Individu spécialisé dans le décryptage des messages chiffrés  
⇒ ennemi du cryptographe
- **Cryptologie** : Branche mathématique s'intéressant au cryptage
- **Chiffrement continu / par blocs** : selon que les données à crypter sont découpées en blocs ou pas

## Equations

- 1  $C = E(M) \leftarrow$  chiffrement
- 2  $D(C) = M \leftarrow$  déchiffrement
- 3  $D(E(M)) = M \leftarrow$  Equivalence

# Algorithmes cryptographiques

## Types d'algos:

- algo = fonction mathématique utilisée pour le chiffrement/déchiffrement
- Deux types d'algo : algo secret<sup>a</sup> et algo public

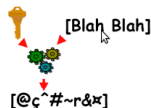
<sup>a</sup>encore appelé algo restreint, n'est quasiment plus le cas aujourd'hui

## Algo restreint

- Réalisation de systèmes sûrs
- Moindre "fuite" au niveau algo détruit toute la sécurité
- Pas de standardisation possible  $\Rightarrow$  pas de compatibilité/interopérabilité

## Algo public

- Sont connus de tous
- Recours à une information "secrete" constituée par une ou plusieurs clés
- En cas de fuite au niveau de la clé, tout le système n'est pas à casser



# Algorithmes cryptographiques

## Types d'algos:

- algo = fonction mathématique utilisée pour le chiffrement/déchiffrement
- Deux types d'algo : algo secret<sup>a</sup> et algo public

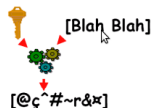
<sup>a</sup>encore appelé algo restreint, n'est quasiment plus le cas aujourd'hui

## Algo restreint

- Réalisation de systèmes sûrs
- Moindre "fuite" au niveau algo détruit toute la sécurité
- Pas de standardisation possible  $\Rightarrow$  pas de compatibilité/interopérabilité

## Algo public

- Sont connus de tous
- Recours à une information "secrete" constituée par une ou plusieurs clés
- En cas de fuite au niveau de la clé, tout le système n'est pas à casser



# Algorithmes cryptographiques

## Types d'algos:

- algo = fonction mathématique utilisée pour le chiffrement/déchiffrement
- Deux types d'algo : algo secret<sup>a</sup> et algo public

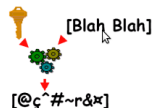
<sup>a</sup>encore appelé algo restreint, n'est quasiment plus le cas aujourd'hui

## Algo restreint

- Réalisation de systèmes sûrs
- Moindre "fuite" au niveau algo détruit toute la sécurité
- Pas de standardisation possible  $\Rightarrow$  pas de compatibilité/interopérabilité

## Algo public

- Sont connus de tous
- Recours à une information "secrete" constituée par une ou plusieurs clés
- En cas de fuite au niveau de la clé, tout le système n'est pas à casser



# Les algorithmes publics...

## ... à clé secrète

- Le destinataire et l'émetteur se mettent d'accord sur une clé (par tout moyen convenable)
- Clé unique pour le chiffrement et le déchiffrement
- Complexité de la clé  $\Rightarrow$  ne doit pas être calculable en un temps raisonnable
- Noeud de la fiabilité du système : Moment de l'échange de la clé

## ... à clé public

- Une clé de chiffrement est communiquée à tous les destinataires potentiels
- La clé publique de chiffrement est associée d'une clé privée connue du seul destinataire
- Principe mathématique fait que la clé privée ne peut être déduite connaissant la clé publique

# Les algorithmes publics...

## ... à clé secrète

- Le destinataire et l'emetteur se mettent d'accord sur une clé (par tout moyen convenable)
- Clé unique pour le chiffrement et le déchiffrement
- Complexité de la clé  $\Rightarrow$  ne doit pas etre calculable en un temps raisonnable
- Noeud de la fiabilité du système : Moment de l'échange de la clé

## ... à clé public

- Une clé de chiffrement est communiquée à tous les destinataires potentiels
- La clé publique de chiffrement est associée d'une clé privée connue du seul destinataire
- Principe mathématique fait que la clé privée ne peut être déduite connaissant la clé publique

# Les algorithmes publics...

## ... à clé secrète

- Le destinataire et l'emetteur se mettent d'accord sur une clé (par tout moyen convenable)
- Clé unique pour le chiffrement et le déchiffrement
- Complexité de la clé  $\Rightarrow$  ne doit pas etre calculable en un temps raisonnable
- Noeud de la fiabilité du système : Moment de l'échange de la clé

## ... à clé public

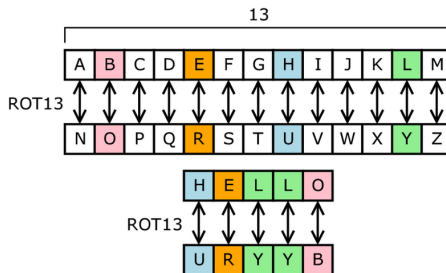
- Une clé de chiffrement est communiquée à tous les destinataires potentiels
- La clé publique de chiffrement est associée d'une clé privée connue du seul destinataire
- Principe mathématique fait que la clé privée ne peut être déduite connaissant la clé publique



# Méthodes cryptographiques simples (1)

## Chiffres à substitution

- Principe: Un symbole est simplement remplacé par un ou plusieurs autres
- Chiffrement à substitution **monoalphabétique** :
  - Plus ancienne et plus simple
  - En général, Remplacer une lettre de l'alphabet par une autre suivant une "règle secrete"
  - E.g., Chiffre de Jules César : Remplacer une lettre par celle se trouvant N places plus loin dans l'alphabet
- Chiffrement à substitution **polyalphabétique**



# Méthodes cryptographiques simples (2)

## Chiffres à substitution

- Principe: Un symbole est simplement remplacé par un ou plusieurs autres
- Chiffrement à substitution **monoalphabétique**
- Chiffrement à substitution **polyalphabétique** :
  - Les chiffres à substitution sont facilement cassables grâce à une analyse des fréquences (e.g., E est courant en français)
  - Avant l'avènement de l'informatique, il fallait déjà augmenter la complexité. (e.g., faire varier la valeur du chiffre N de César)
  - Carré de Vigenere : Simplifier le cryptage et le décryptage... mais pas la complexité de la clé

Clé	C	A	R	T	E	S	A	P	U	C	E	C	A	R	T
Clair	U	T	I	L	I	S	A	T	I	O	N	D	U	C	H
Crypté	W	T	Z	E	M	K	A	I	C	Q	R	F	U	T	A

Clé	E	S	A	P	U	C	E	C	A	R	T	E	S	A	P
Clair	I	F	F	R	E	D	E	V	I	G	E	N	E	R	E
Crypté	M	X	F	G	Y	B	I	X	I	X	X	J	W	R	T

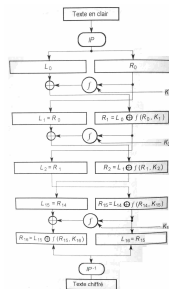
Clair	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
26	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

# Algorithmes cryptographiques complexes... (1)

... à clé secrète

- DES/DEA: *Data Encryption Stantard/Algorithm*

- Algo de chiffrement par blocs (64bits)
- Clé de 56 bits en fait + 8bits (inutilisé ou de parité)
- Normalisation permet d'avoir des modules prêts à l'emploi pour la carte à puce
- Un meme algo pour le chiffrement et le décryptage



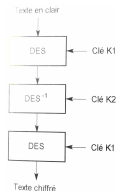
## Sécurité & Programmation

- Certains ont déjà enterré le DES, car l'algorithme s'est avéré cassable...
- ... si on y met les ressources et le temps nécessaires ( $2^{47}$  essais de clé)
- Beaucoup d'implémentations gratuites existent (e.g., <http://us.cryptosoft.de/html/home.htm>)

# Algorithmes cryptographiques complexes... (2)

... à clé secrète

- DES/DEA: *Data Encryption Standard/Algorithm*
- triple DES: *triple Data Encryption Standard*
  - Enchaînement de 3 DES successifs
  - 2 clés distincts pour 2 chiffrements et 1 décryptage
  - Clé de 56 bits en fait + 8bits (inutilisé ou de parité)



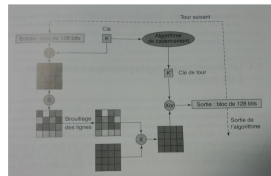
## Sécurité & Programmation

- Réputé inviolable jusqu'à présent
- Théoriquement, il faut pouvoir essayer environ  $2^{56}$  DES consécutifs pour en venir à bout  
e.g., si jamais on construit une machine qui casse 1 DES à la seconde, il lui faudra 2,2 milliards années
- Prb: le triple DES est 3 fois plus lent qu'un DES...

# Algorithmes cryptographiques complexes... (3)

... à clé secrète

- DES/DEA: *Data Encryption Stantard/Algorithm*
- triple DES: *triple Data Encryption Stantard*
- AES: *Advanced Data Encryption Stantard*
  - Algo de chiffrement par blocs (128 bits)
  - Sécurité absolue avec une clé de 128 bits
  - Facile à mettre en oeuvre (matériel et logiciel)
  - Algo rapide (6x plus rapide qu'un DES malgré une clé 2x plus longue)
  - Algo sûr résistant à toutes les techniques de cryptanalyse



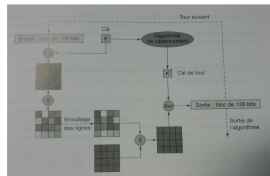
## Sécurité & Programmation

- $2^{128}$  secondes = 150.000 milliards années pour casser un AES  
(notre univers a seulement 20 milliards d'années)
- L'AES est cependant plus rare que le triple DES sur les cartes à puces actuelles

# Algorithmes cryptographiques complexes... (4)

## ... à clé publique

- **RSA: Ron Rivest, Adi Shamir, Leonard Adleman**
  - Algo de chiffrement par blocs (128 bits)
  - Sécurité absolue avec une clé de 128 bits
  - Facile à mettre en oeuvre (matériel et logiciel)
  - Algo rapide (6x plus rapide qu'un DES malgré une clé 2x plus longue)
  - Algo sûr résistant à toutes les techniques de cryptanalyse



## Sécurité & Programmation

- $2^{128}$  secondes = 150.000 milliards années pour casser un AES  
(notre univers a seulement 20 milliards d'années)
- L'AES est cependant plus rare que le triple DES sur les cartes à puces actuelles