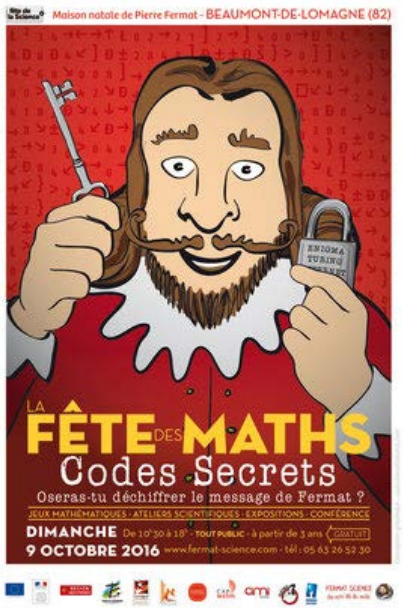
Sobriété numérique et sécurité (cryptographie) : comment concilier cela ?
La cryptographie au service des citoyens

Jean-Jacques Quisquater
UCL Crypto Group
Louvain-la-Neuve Belgique
jjq@uclouvain.be
25 septembre 2020



- Sobriété numérique et sécurité (cryptographie) : comment concilier cela ?

- résumé :
- Nous expliquerons d'abord ce qu'est la cryptographie et ses différents usages. Nous verrons aussi ce que peut être la sobriété numérique dans tous ses états. Nous verrons alors qu'il peut y avoir contradiction car beaucoup d'algorithmes cryptographiques sont fort gourmands. De plus, les ordinateurs quantiques pouvant arriver, il prévu très vite, 2022, d'appuyer de nouveaux algorithmes, encore plus gourmands. Enfin, il y a aussi, dans le domaine de l'informatique, presque contradiction entre obsolescence matérielle et logicielle et meilleure sécurité IT.

Sobriété numérique

- Voir https://theshiftproject.org/article/rapport-intermediaire-deployer-sobriete-numerique/ (janvier 2020)

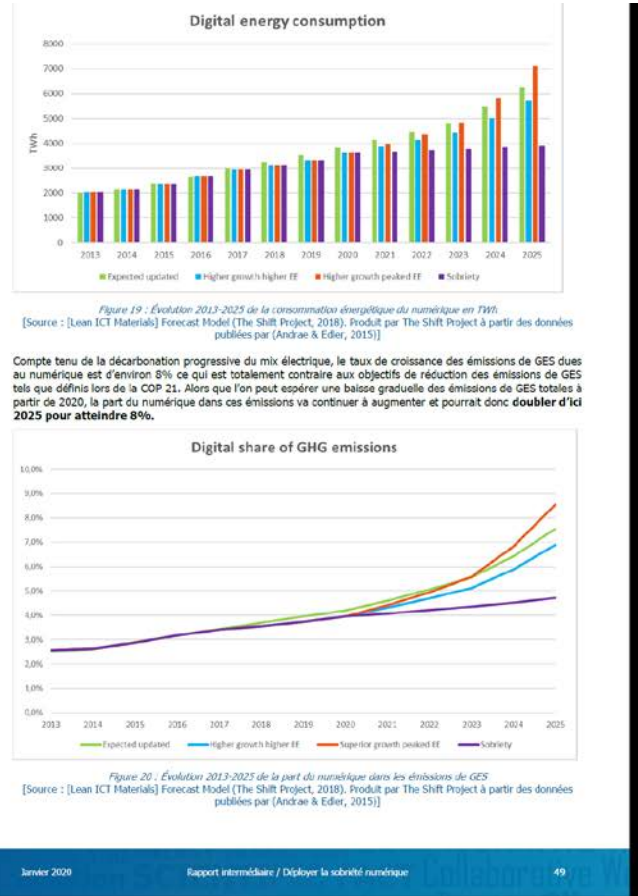


Figure 19 : Évolution 2013-2025 de la consommation énergétique du numérique en TWh
[Source : [Lean ICT Materials] Forecast Model (The Shift Project, 2018). Produit par The Shift Project à partir des données publiées par (Andrae & Edler, 2015)]

Compte tenu de la décarbonation progressive du mix électrique, le taux de croissance des émissions de GES dues au numérique est d'environ 8% ce qui est totalement contraire aux objectifs de réduction des émissions de GES tels que définis lors de la COP 21. Alors que l'on peut espérer une baisse graduelle des émissions de GES totales à partir de 2020, la part du numérique dans ces émissions va continuer à augmenter et pourrait donc **doubler d'ici 2025 pour atteindre 8%.**

Figure 20 : Évolution 2013-2025 de la part du numérique dans les émissions de GES
[Source : [Lean ICT Materials] Forecast Model (The Shift Project, 2018). Produit par The Shift Project à partir des données publiées par (Andrae & Edler, 2015)]

CARBONALYSER

Carbonalyser

par The Shift Project

Analyse Internet usage carbon footprint

Retirer

⚠ This add-on is not actively monitored for security by Mozilla. Make sure you trust it before installing. En savoir plus

4 441 Utilisateurs	33 Critiques	4,8 étoiles

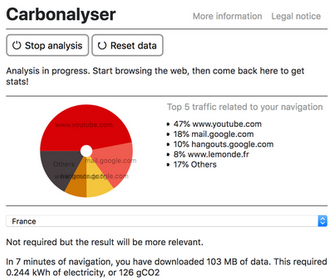
5 ★		26
4 ★		7
3 ★		0
2 ★		0
1 ★		0

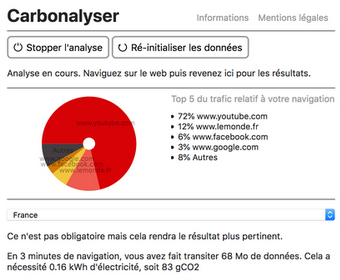
Évaluez votre expérience

Est-ce que **Carbonalyser** vous plait ?

Connectez-vous pour noter cette extension

Captures d'écran



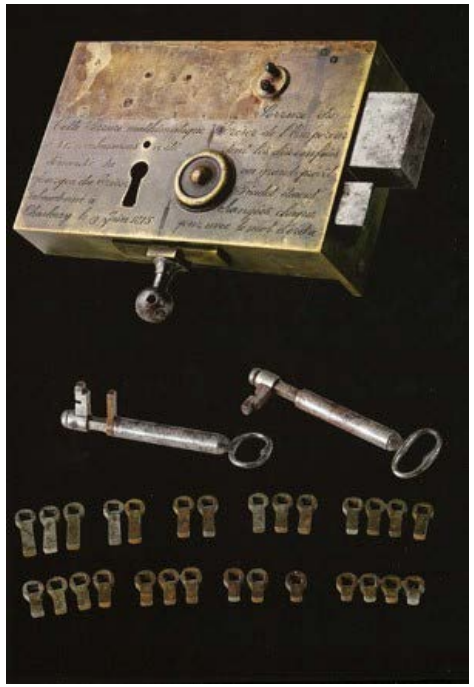


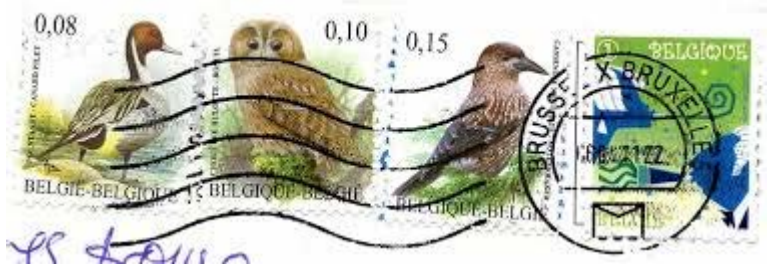
Cryptographie pour tous

- Le citoyen aujourd'hui rencontre dans son quotidien l'usage de la cryptographie.
- C'est l'équivalent informatique des serrures et des coffres-forts, des enveloppes scellées et de la signature manuelle. Nous voulons ici de façon très pédagogique faire comprendre les mécanismes fondamentaux de la cryptographie dans ses usages qui concernent vraiment tous. Il s'agit aussi d'en appréhender les limites, les contraintes, les solutions qu'elle apporte à des problèmes qui semblent pourtant sans solution.
- Nous parlerons aussi du vote électronique où la cryptographie apporte des nouvelles visions intéressantes (ne pas confondre avec le vote électronique tel qu'il est pratiqué en Wallonie et qui est complètement dépassé).
- Nous évoquerons les problèmes de la cryptographie quant à double usage : c'est aussi, bien sûr, comme presque toutes les technologies, utilisé pour des buts bien moins nobles que protéger le commerce électronique ou la vie privée : il s'agit ici des ransomwares, du dark web, etc.

La cryptographie au service du citoyen

- comment sont protégés les cartes de paiement, les passeports, Internet…

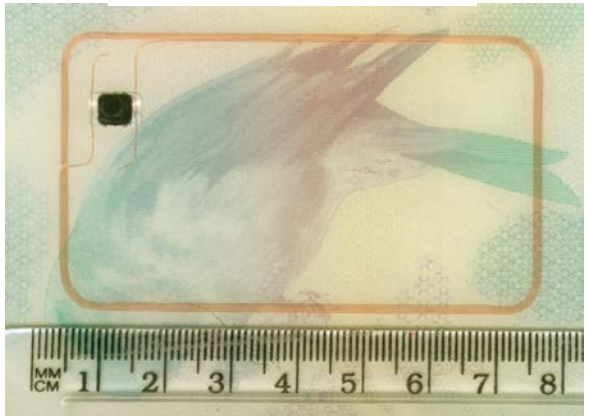





Standard Chartered
123456
5149 1612 3456 7890
PLATINUM
5149
VALID TO: 01/08
DARYL TAN
MasterCard
1 2 3 4 5 C
6 7 8 9 0 OK
ON/OFF
OTP
SIGN


BELGIQUE
BELGIË
BELGIEN
Gates
William Henry
Seattle (Washington) 28 OCT 1955
US citizen
31.01.2005 - 31.01.2010
Bill Gates


UNION EUROPEENNE
EUROPESE UNIE
EUROPÄISCHE UNION
ROYAUME DE BELGIQUE
KONINKRIJK BELGIE
KÖNIGREICH BELGIEN
PASSEPORT - PASPOORT - REISEPASS


MM
CM
1 2 3 4 5 6 7 8


Wi Fi


HTTPS://WWW

Internet – web - chronologie

- Internet : 1969 (ARPA)
- Premier email : 1971 (utilisation aussi de @) : etiquette
  - Premier spam : 1978
- Premier email en Belgique : autour de 1980
- Premier virus : 1983 (Cohen et Adleman) : 1982 (Elk Clooner)
- Noms de domaine (.com, .net, .org, …) : 1985
- Premier worm : 1988 : 1971 (creeper)
- Première page web : 1990 (CERN)
- Amazon : 1994
- Premier phishing : 1995
- Ebay : 1995
- Google : 1998
- Wikipedia : 2001
- Linkedin : 2003
- Facebook : 2004
- Twitter : 2006
- Snapchat : 2011

- https://www.webfx.com/internet-real-time/
- https://www.internetlivestats.com/
- https://visual.ly/community/Infographics/how/internet-real-time
- https://www.electricitymap.org/map
- https://www.electricitymap.org/zone/BE?wind=true&solar=false
- https://www.betfy.co.uk/internet-realtime/

Belgique :

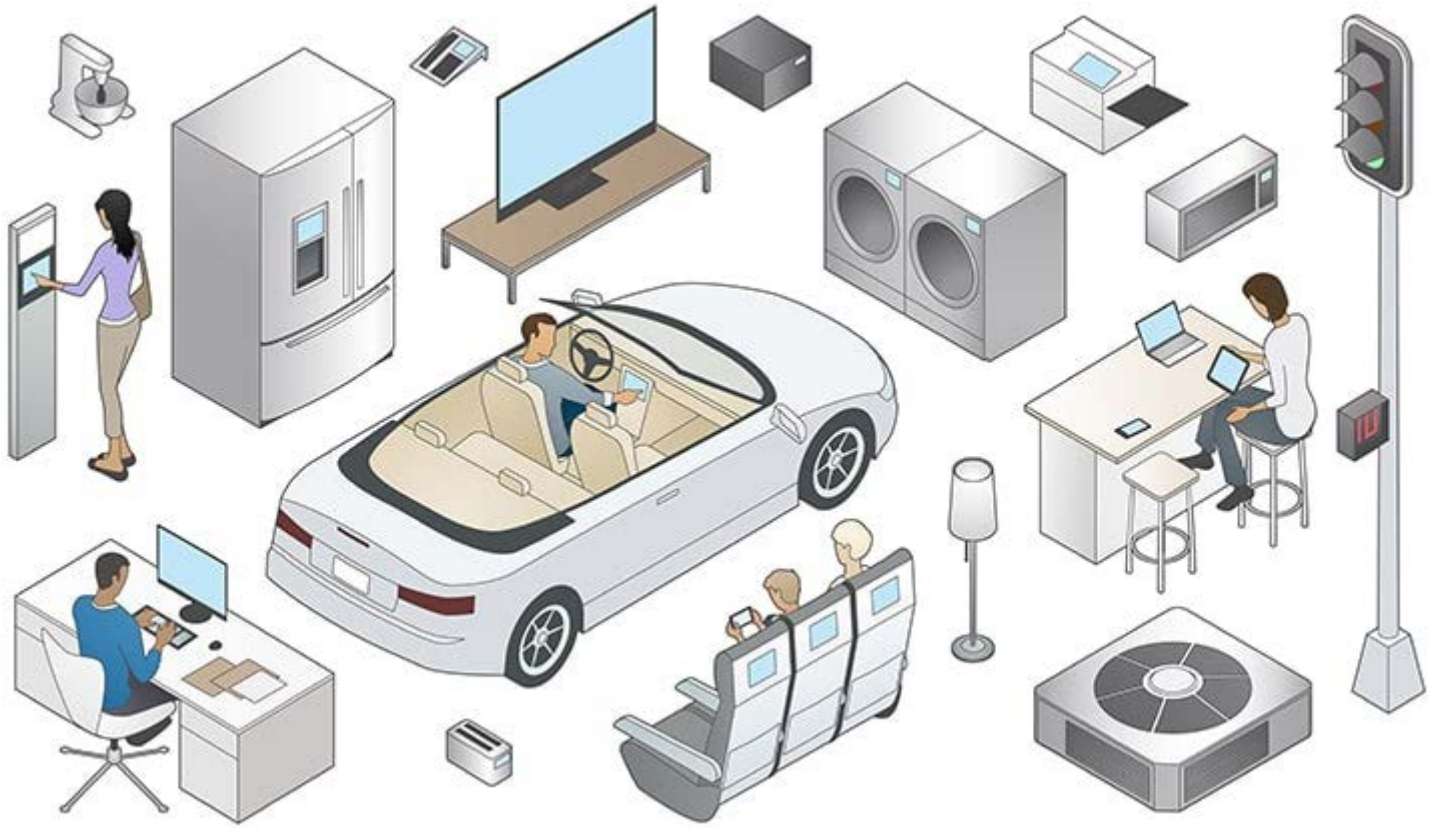
Internet Usage and Population Statistics:

YEAR	Users	Population	% Pop.	Usage Source
2000	2,000,000	10,250,995	19.5 %	ITU
2004	3,769,123	10,355,844	36.4 %	Nielsen NetRatings
2006	5,100,000	10,516,112	48.5 %	C. I. Almanac
2009	7,292,300	10,414,336	70.0 %	I. T. U.
2010	8,113,200	10,423,493	77.8 %	I. T. U.
2012	8,489,901	10,438,353	81.3 %	I. W. S.
2014	9,441,116	11,258,434	83.9 %	I. W. S.
2015	9,569,669	11,258,434	85.0 %	I. W. S.

Internet Users in the European Union - 2016

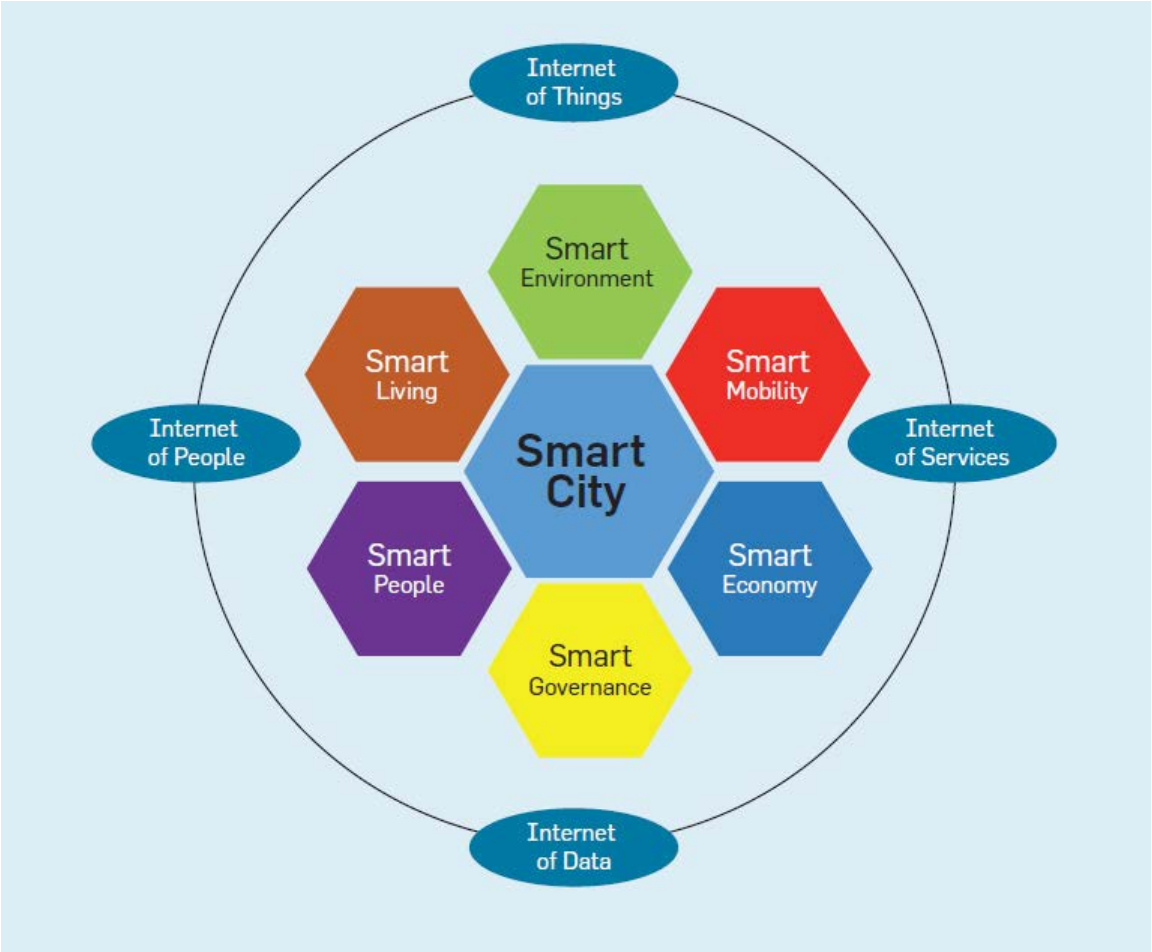
EUROPEAN UNION	Population (2016 Est.)	Internet Users, 30-June-2016	Penetration (% Population)	Users % Table	FACEBOOK 30-June-2016
Austria	8,584,926	**7,135,168**	83.1 %	1.8 %	3,500,000
Belgium	11,258,434	**9,569,669**	85.0 %	2.4 %	5,900.000
Bulgaria	7,202,198	**4,083,950**	56.7 %	1.0 %	3,200,000
Croatia	4,225,316	**3,167,838**	75.0 %	0.8 %	1,800,000
Cyprus	847,008	**804,306**	95.0 %	0.2 %	590,000
Czech Republic	10,538,275	**8,400,059**	79.7 %	2.1 %	4,500,000
Denmark	5,659,715	**5,432,760**	96.0 %	1.3 %	3,500,000
Estonia	1,313,271	**1,106,299**	84.2 %	0.3 %	590,000
Finland	5,471,753	**5,117,660**	93.5 %	1.3 %	2,600,000
France	66,132,169	**55,429,382**	83.8 %	13.8 %	32,000,000
Germany	81,174,000	**71,727,551**	88.4 %	17.8 %	29,000,000
Greece	10,812,467	**6,834,560**	63.2 %	1.7 %	4,800,000
Hungary	9,849,000	**7,498,044**	76.1 %	1.9 %	5,100,000
Ireland	4,625,885	**3,817,491**	82.5 %	0.9 %	2,600,000
Italy	60,795,612	**37,668,961**	62.0 %	9.3 %	28,000,000
Latvia	1,986,096	**1,628,854**	82.0 %	0.4 %	650,000
Lithuania	2,921,262	**2,399,678**	82.1 %	0.6 %	1,400.000
Luxembourg	562,958	**532,952**	94.7 %	0.1 %	280,000
Malta	429,344	**314,151**	73.2 %	0.1 %	270,000
Netherlands	16,900,726	**16,143,879**	95.5 %	4.0 %	9,500,000
Poland	38,005,614	**25,666,238**	67.5 %	6.4 %	14,000,000
Portugal	10,374,822	**7,015,519**	67.6 %	1.7 %	5,600,000
Romania	19,861,408	**11,178,477**	56.3 %	2.8 %	8,100,000
Slovakia	5,421,349	**4,507,849**	83.1 %	1.1 %	2,300,000
Slovenia	2,062,874	**1,501,039**	72.8 %	0.4 %	850,000
Spain	46,439,864	**35,705,960**	76.9 %	8.9 %	22,000,000
Sweden	9,747,355	**9,216,226**	94.6 %	2.3 %	5,600,000
United Kingdom	64,767,115	**59,333,154**	91.6 %	14.7 %	38,000,000

Internet des objets




IoT Hardware Enabled Cryptography
TV
MICROCHIP
CEC1302

Smart city


Internet of Things
Smart Environment
Smart Living
Smart Mobility
Internet of People
Smart City
Internet of Services
Smart People
Smart Economy
Smart Governance
Internet of Data

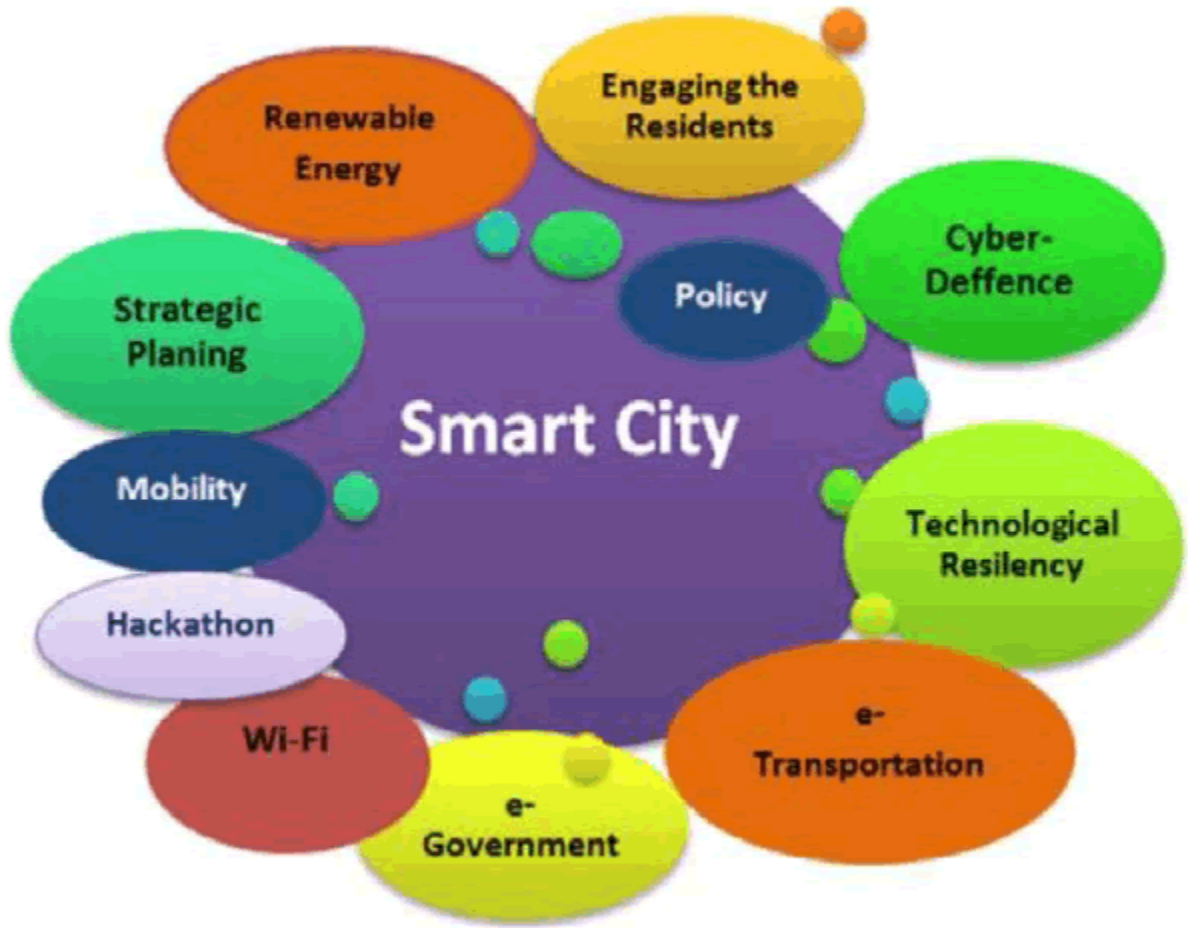
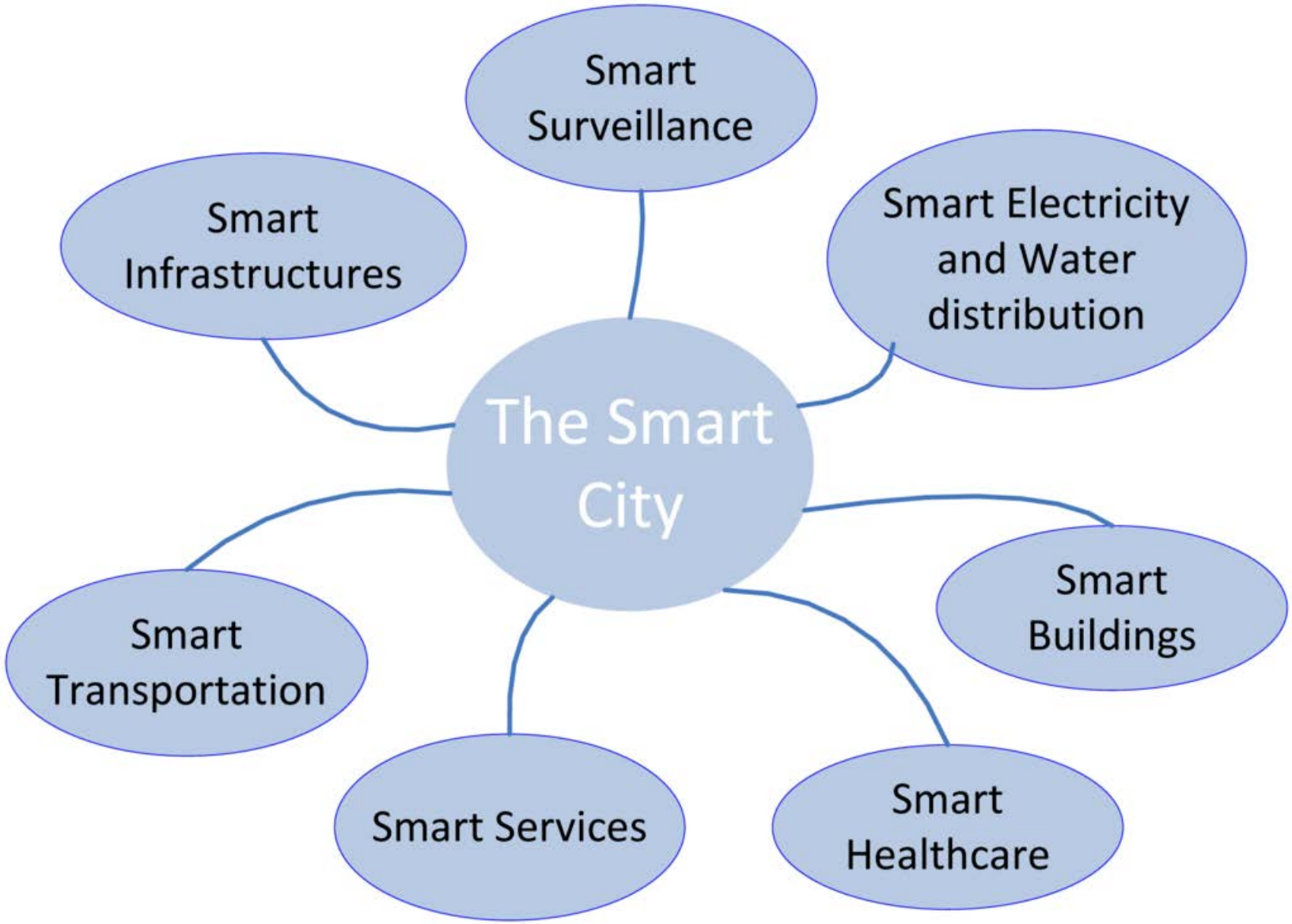


Figure 2: Integrated sectors in a smart city.


Smart Surveillance
Smart Infrastructures
Smart Electricity and Water distribution
The Smart City
Smart Transportation
Smart Buildings
Smart Services
Smart Healthcare

Rôle de la cryptographie citoyenne : propager et renforcer la confiance

- Protéger la vie privée quand cela est nécessaire,
- Assurer la preuve de l'origine des fichiers et, même, des biens,
- Être vérifiable par toutes et tous,
- Éviter les copies illicites, non voulues par leurs créateurs,
- Attribuer à chacun ce qui lui est dû,

- Dans le cadre d'une économie voulue, de plus en plus numérique.

Codes secrets et cryptographie

- Une longue histoire,
- Plutôt un art très longtemps,
- Albert (1941) et Shannon (1943-1949) introduisent la théorie mathématique des systèmes à clé secrète,
- Diffie-Hellman-Merkle (1975) inventent les systèmes à clé publique,
- Rivest-Shamir-Adleman (1977 : RSA) utilisent la théorie de Fermat (1640) pour produire du chiffrement t des signatures digitales,
- Du moins, c'est l'histoire officielle …

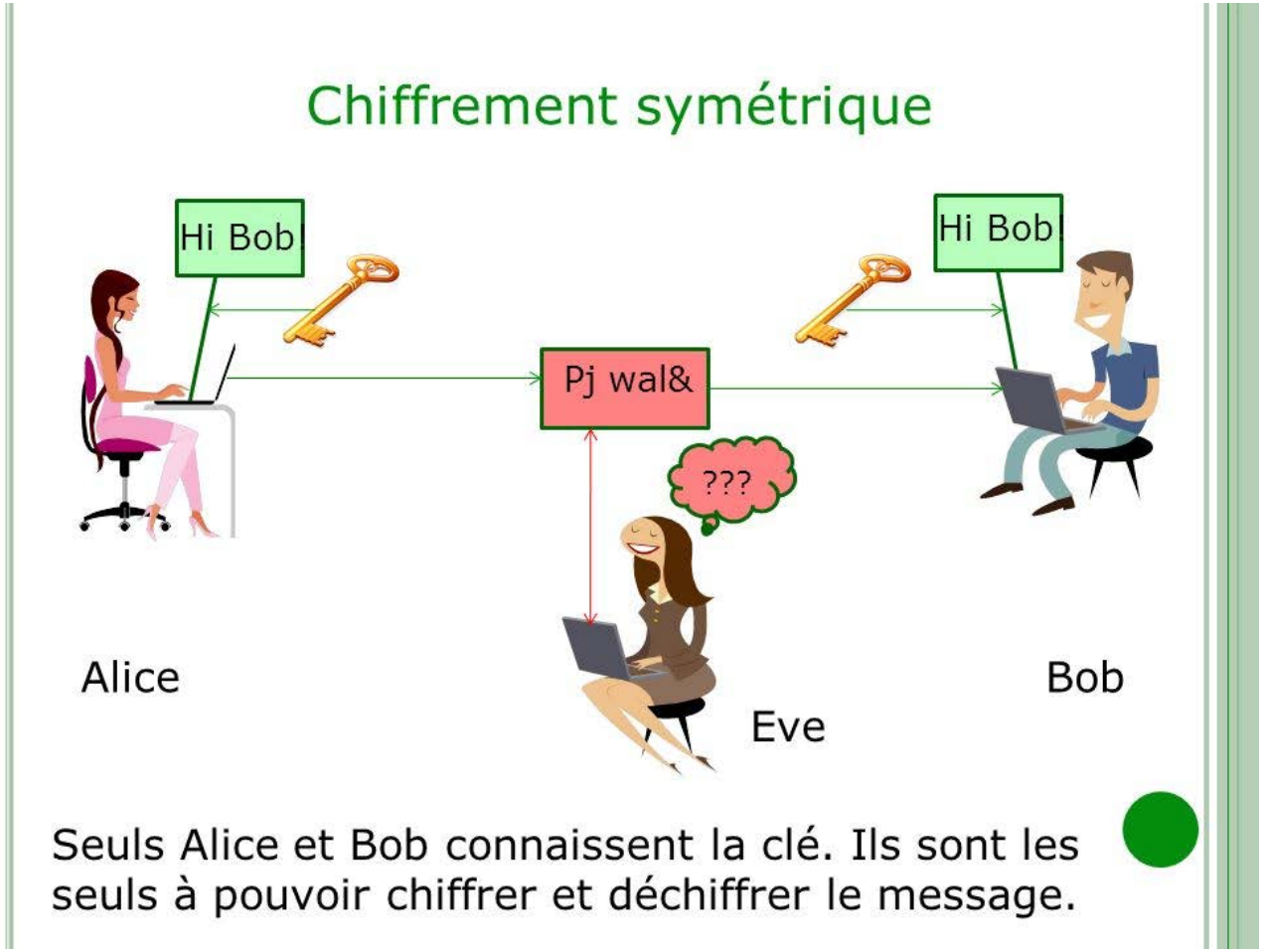
Que protéger ?

- Courrier électronique,
- Commerce électronique,
- Vie privée,
- Secret médical,
- Véracité des informations,
- Intégrité des archives,
- Confiance,
- Vote, ?
- …

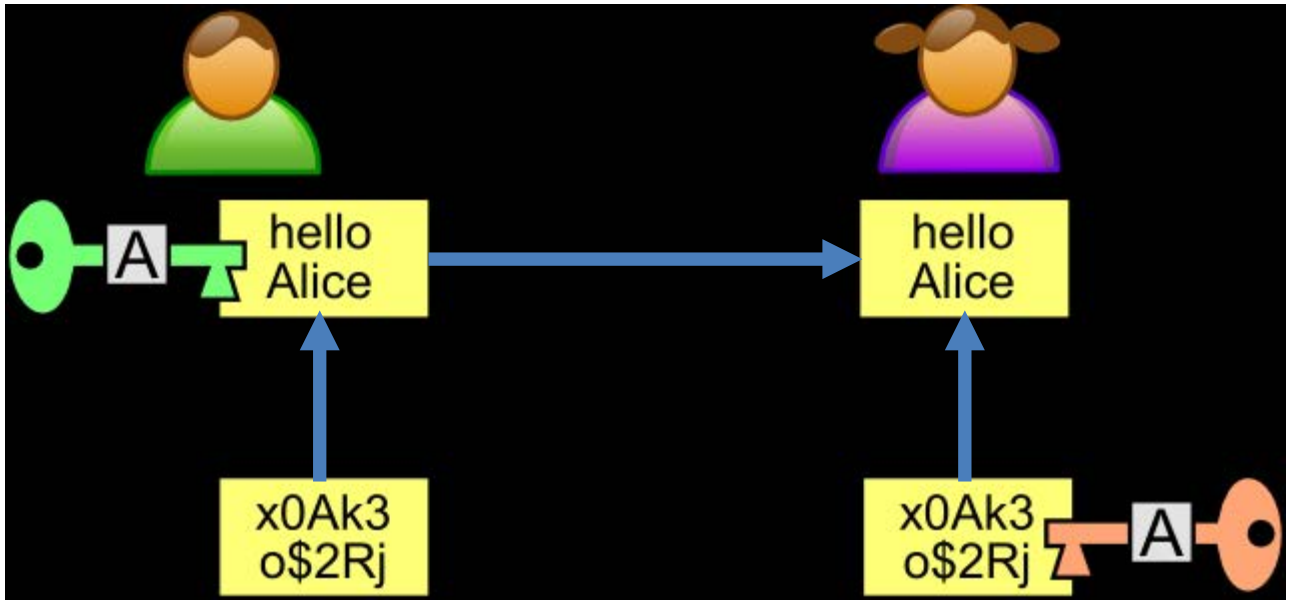
Cryptographie - sécurité

- Confidentialité : chiffrement,
- Intégrité : signature,
- Authentification : identification,
- Anonymat :
- Disponibilité.

chiffrement



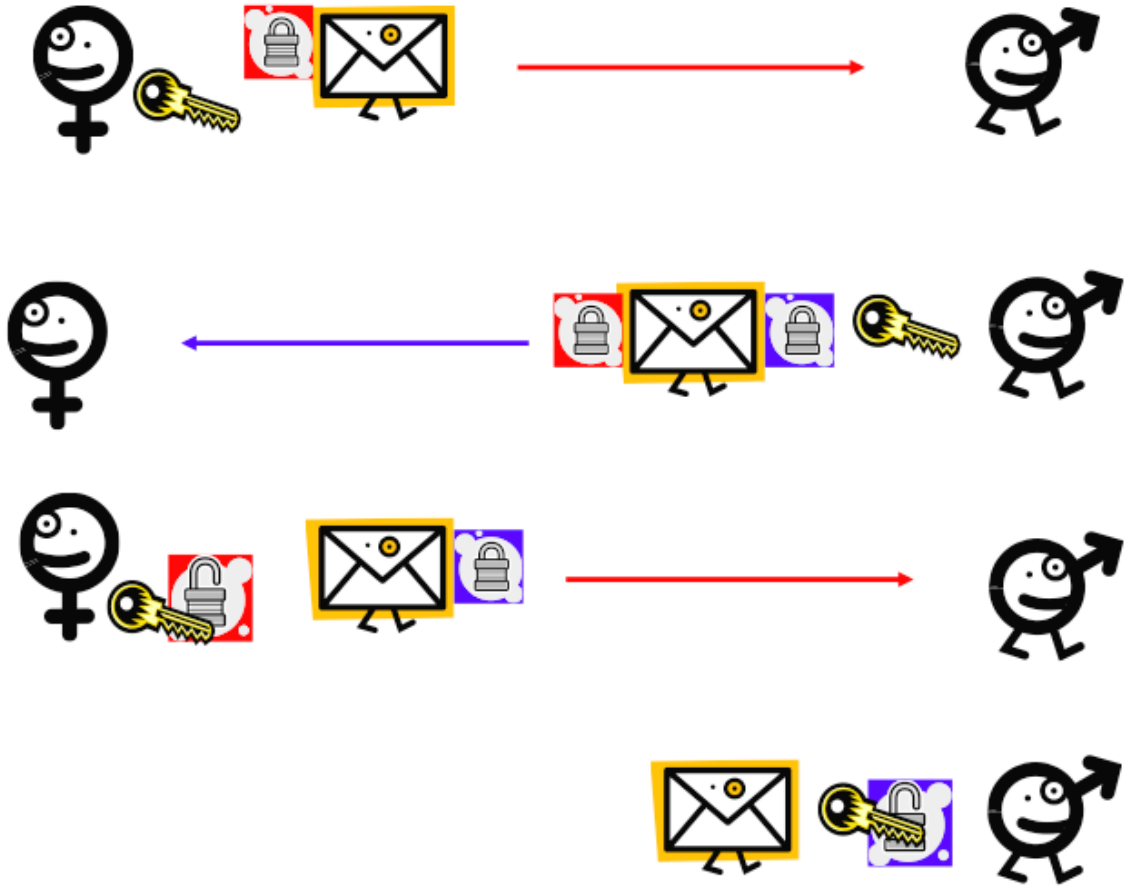
Clé publique et clé accélératrice



Coffre, cadenas, clé …

- Transport sécurisé d’un message par clé secrète,
- Transport sécurisé avec cadenas ouvert (et public),
- Distribution de clé (trois échanges),

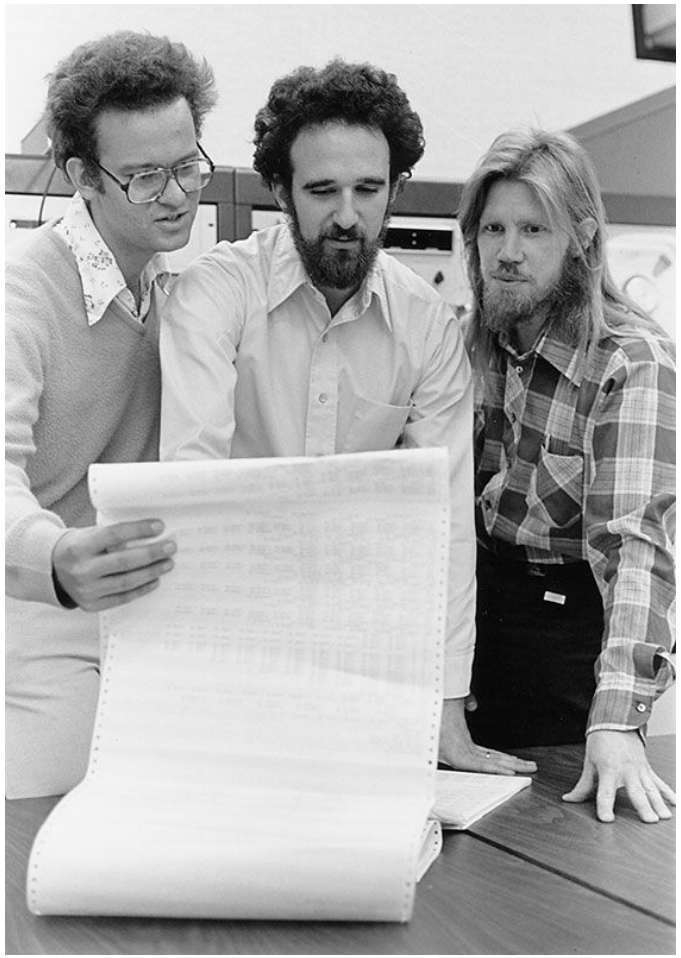
Clés secrètes, clés publiques … :
transport sécurisé d'une lettre : chacun garde sa clé :
protocole des deux cadenas



problème

- S’il y a un pirate, que peut-il faire ?
- Intercepter le colis au premier échange et mettre son cadenas à la place …
- Il y a des variantes où le pirate échange d’abord avec A puis avec B en copiant la clé échangée.

Cryptographie à clé publique : Diffie-Hellman-Merkle (1976)



Invited Paper

Whitfield Diffie and Martin E. Hellman

Abstract Two kinds of contemporary developments in cryptography are examined. Widening applications of teleprocessing have given rise to a need for new types of cryptographic systems, which minimize the need for secure key distribution channels and supply the equivalent of a written signature. This paper suggests ways to solve these currently open problems. It also discusses how the theories of communication and computation are beginning to provide the tools to solve cryptographic problems of long standing.

1 INTRODUCTION

We stand today on the brink of a revolution in cryptography. The development of cheap digital hardware has freed it from the design limitations of mechanical computing and brought the cost of high grade cryptographic devices down to where they can be used in such commercial applications as remote cash dispensers and computer terminals. In turn, such applications create a need for new types of cryptographic systems which minimize the necessity of secure key distribution channels and supply the equivalent of a written signature. At the same time, theoretical developments in information theory and computer science show promise of providing provably secure cryptosystems, changing this ancient art into a science.

The development of computer controlled communication networks promises effortless and inexpensive contact between people or computers on opposite sides of the world, replacing most mail and many excursions with telecommunications. For many applications these contacts must be made secure against both eavesdropping and the injection of illegitimate messages. At present, however, the solution of security problems lags well behind other areas of communications technology. Contemporary cryptography is unable to meet the requirements, in that its use would impose such severe inconveniences on the system users, as to eliminate many of the benefits of teleprocessing.

The best known cryptographic problem is that of privacy: preventing the unauthorized extraction of information from communications over an insecure channel order to use cryptography to insure privacy, however, it currently necessary for the communicating parties to share a key which is known to no one else. This is done by sending the key in advance over some secure channel such a private courier or registered mail. A private conversation between two people with no prior acquaintance is a common occurrence in business, however, and it is unrealistic to expect initial business contacts to be postponed long enough for keys to be transmitted by some physical means. The cost and delay imposed by this key distribution problem is a major barrier to the transfer of business communications to large teleprocessing networks.

Section III proposes two approaches to transmitting keying information over public (i.e., insecure) channel without compromising the security of the system. In *public key cryptosystem* enciphering and deciphering are governed by distinct keys, E and D, such that computing D from E is computationally infeasible (e.g., requiring 10^{100} instructions). The enciphering key E can thus be publicly disclosed without compromising the deciphering key D. Each user of the network can, therefore, place his enciphering key in a public directory. This enables any user of the system to send a message to any other user enciphered in such a way that only the intended receiver is able to decipher it. As such, a public key cryptosystem is multiple access cipher. A private conversation can therefore be held between any two individuals regardless of whether they have ever communicated before. Each one sends messages to the other enciphered in the receiver public enciphering key and deciphers the messages he receives using his own secret deciphering key.

We propose some techniques for developing public key cryptosystems, but the problem is still largely open.

Public key distribution systems offer a different approach to eliminating the need for a secure key distribution channel. In such a system, two users who wish to exchange a key communicate back and forth until they arrive a key in common. A third party eavesdropping on this exchange must find it computationally infeasible to compute the key from the information overheard. A possible solution to the public key distribution problem is given in Section III, and Merkle [1] has a partial solution of a different form.

A second problem, amenable to cryptographic solution which stands in the way of replacing contemporary business communications by teleprocessing systems is authentication. In current business, the validity of contracts guaranteed by signatures. A signed contract serves as gal evidence of an agreement which

Manuscript received June 3, 1976. This work was partially supported by the National Science Foundation under NSF Grant ENG 10173. Portions of this work were presented at the IEEE Information Theory Workshop, Lenox, MA, June 23–25, 1975 and the IEEE International Symposium on Information Theory in Ronneby, Sweden, June 21–24, 1976.

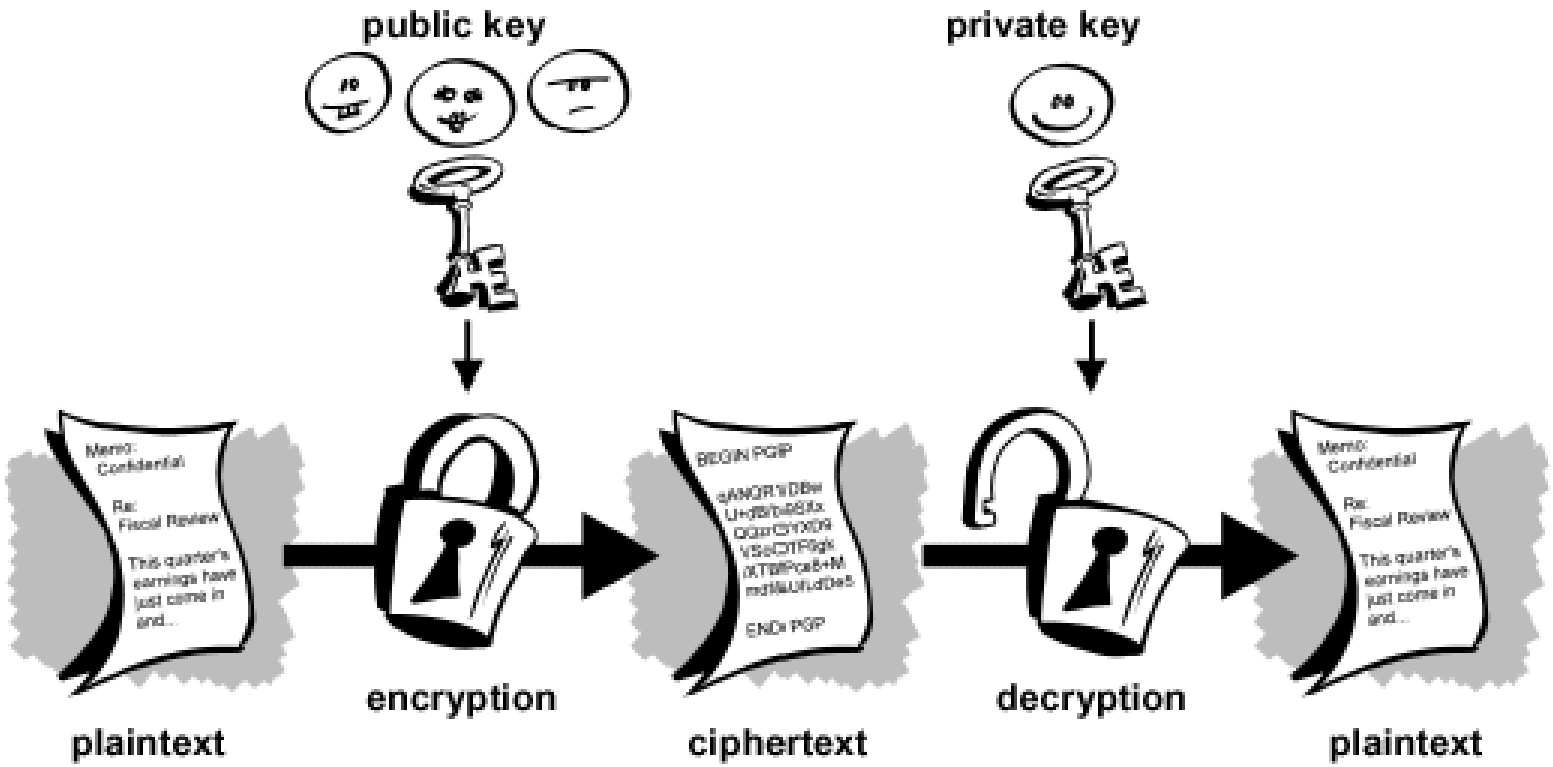
W. Diffie is with the Department of Electrical Engineering, Stanford University, Stanford, CA, and the Stanford Artificial Intelligence Laboratory, Stanford, CA 94305.

M. E. Hellman is with the Department of Electrical Engineering, Stanford University, Stanford, CA 94305.

et déclic pour moi …

- Le début de ma carrière en crypto chez Philips,
- …

Chiffrement par clé publique



RSA

The IEEE Koji Kobayashi Computers and Communications Award :
1999 – 2000
Photo : 21 août 2000 à CRYPTO 2000 (par Eli Biham)

THE SCIENCES

Mathematical Games, August 1977

A new kind of cipher that would take millions of years to break

By Martin Gardner on August 1, 1977 3

PURCHASE TO READ MORE

This article is only available as a PDF.
Already purchased? Sign in to access the full article.

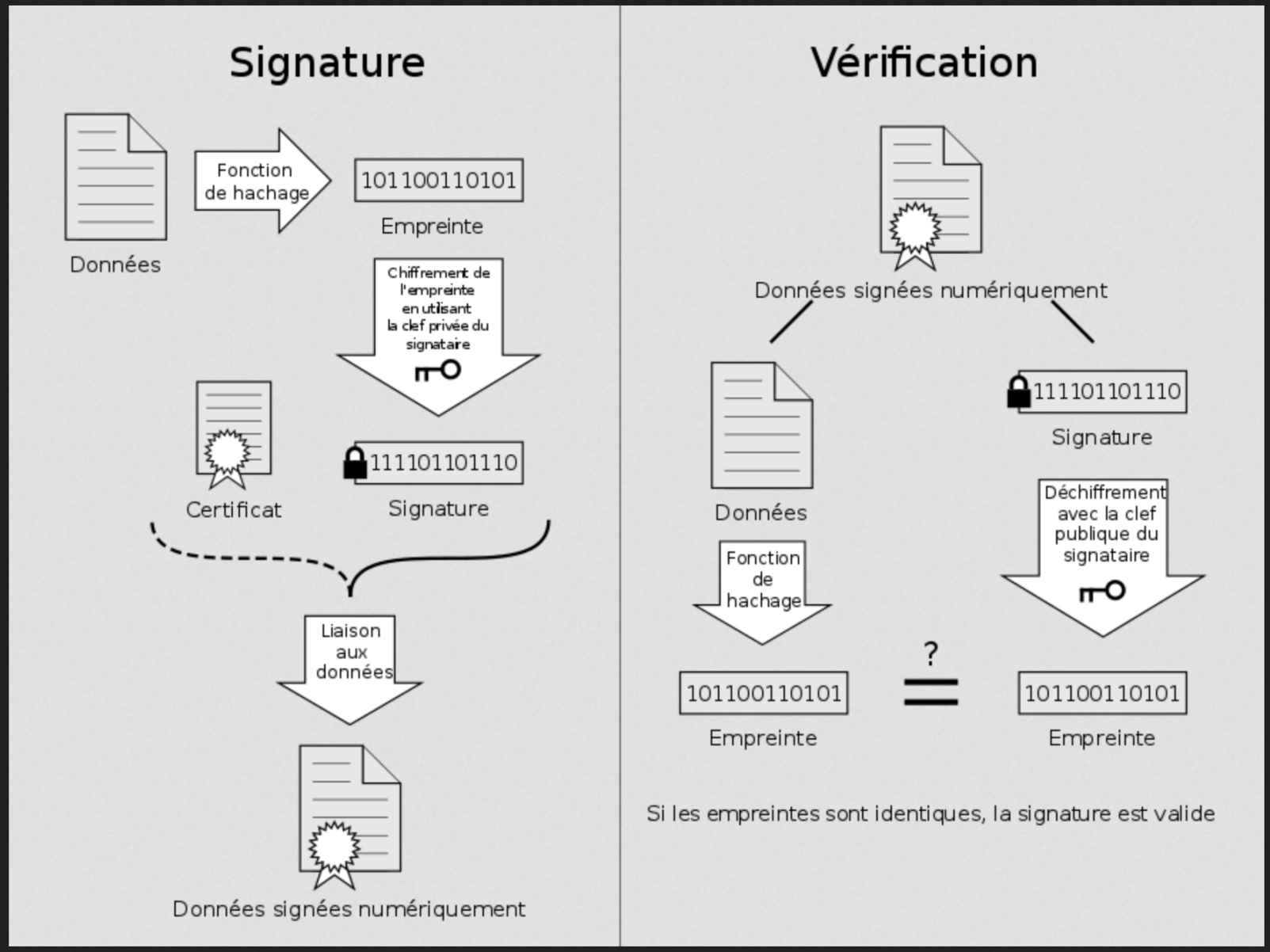
DIGITAL ISSUE ?	$7.99
PRINT + DIGITAL ALL ACCESS SUBSCRIPTION ?	$99.00

La cryptographie a une histoire

- Aux mains d'abord des gouvernements, des diplomates, des militaires et de quelques grands marchands,
- Découvertes civiles fondamentales autour de 1975,
- Débuts difficiles,
- Rendud aux civils en 1999 (USA, France, …) !
- Et avant ?


il n'y a rien de plus beau qu'une clef
(MAURICE MAETERLINCK)
tant qu'on ne sait pas ce qu'elle ouvre
© www. Citations du Monde .com

signatures


Signature
Données
Fonction de hachage
101100110101
Empreinte
Chiffrement de l'empreinte en utilisant la clef privée du signataire
Certificat
111101101110
Signature
Liaison aux données
Données signées numériquement
Vérification
Données signées numériquement
Données
111101101110
Signature
Déchiffrement avec la clef publique du signataire
Fonction de hachage
?
101100110101
Empreinte
101100110101
Empreinte
Si les empreintes sont identiques, la signature est valide

Exemples de fonction à sens unique

- Dictionnaire unique,
- Produit de deux nombres entiers,
- Circulation du sang,
- …

Vos données sur le web ?

- Stocker chiffrer,

- Interroger sans déchiffrer ?

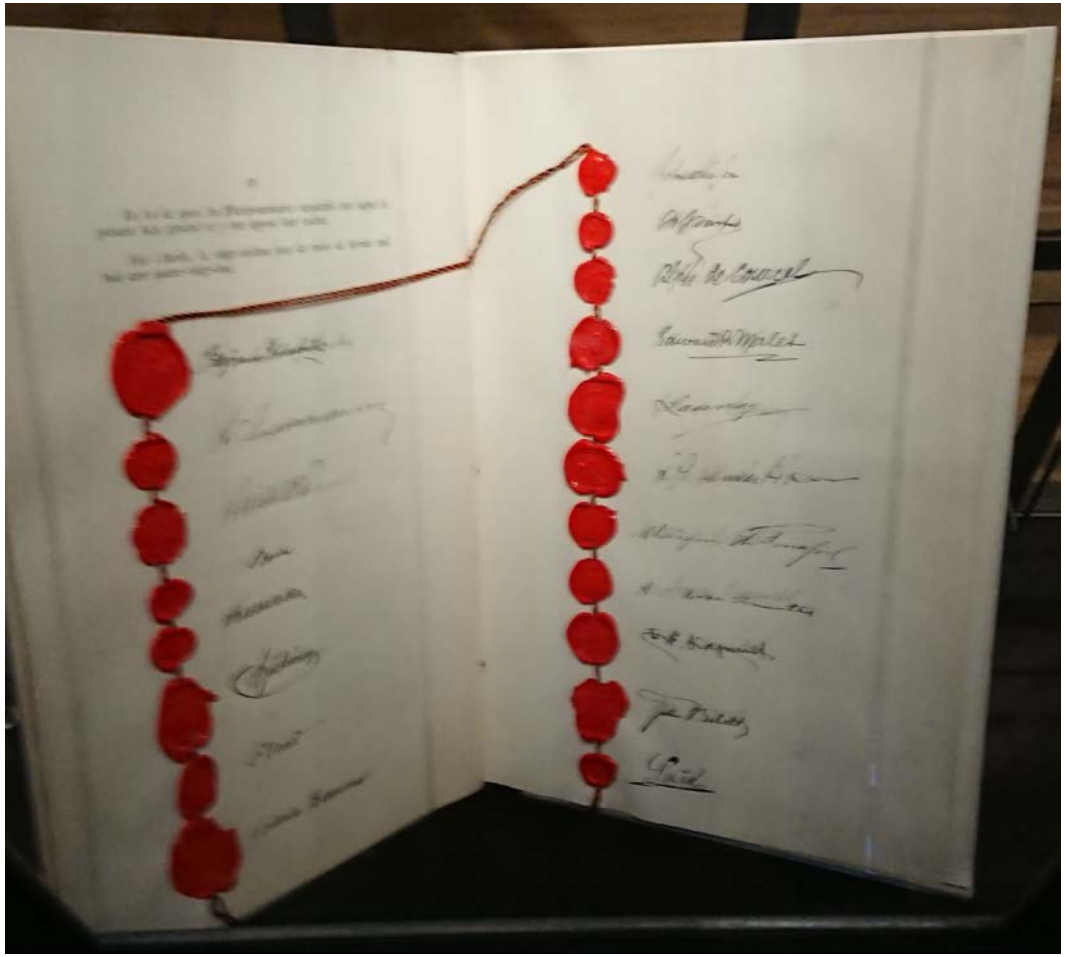
Vote électronique

- Pouvoir compter en ne donnant que le total
- Problèmes délicats dépendant du contexte
- Peut améliorer le vote si mixte (= électronique + papier)

Dark web - ransomware

- Utilisation de Tor (logiciel pour renforcer l’anonymat
- Chiffrement de vos fichiers pour vous rançonner

Bitcoin - blockchain



Cryptographie quantique

- Deux domaines,
- Réaliser,
- Attaquer : ordinateurs quantiques,
- Changement : nouveaux algorithmes pour 2022,
- Plus gourmand ? Changer les interfaces …

Obsolescence …

- Garder plus longtemps,
- Mais risque de sécurité, d’impossibles mises à jour,
- Incompatibilité,

- Pourrait être plus coûteux que la mise à jour pour le bug de l’an 2000.

Usage de la cryptographie

- Impossibilité de comprimer, si de bout en bout,
- Visioconférence chiffrée complète : très coûteux à cause du chiffrement local,
- Le chiffrement consomme,
- Problème pour l’IoT.