

Ces protocoles qui nous protègent ...

STÉPHANIE DELAUNE

Chargée de Recherche CNRS affectée au LSV
Équipe-Projet SecSI



L'enseignement en informatique à l'ENS Cachan

→ formation tournée vers les **fondements de l'informatique**



L'enseignement en informatique à l'ENS Cachan

- > formation tournée vers les **fondements de l'informatique**
- ▶ **Les bases:** calculabilité et logique, algorithmique, complexité, langages formels, programmation, ...
 - ▶ **Des enseignements plus poussés:** preuves assistées par ordinateur, démonstration automatique, bioinformatique, ...

L'enseignement en informatique à l'ENS Cachan

- formation tournée vers les **fondements de l'informatique**
- ▶ **Les bases:** calculabilité et logique, algorithmique, complexité, langages formels, programmation, ...
 - ▶ **Des enseignements plus poussés:** preuves assistées par ordinateur, démonstration automatique, bioinformatique, ...

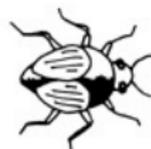
« La science informatique n'est pas plus la science des ordinateurs que l'astronomie n'est celle des télescopes »

E. Dijkstra



La recherche au LSV

Ennemi public numéro 1: le **bug** !



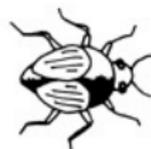
La recherche au LSV

Ennemi public numéro 1: le **bug** !



→ accroître notre confiance dans les **logiciels critiques**

Ennemi public numéro 1: le bug !



—> accroître notre confiance dans les logiciels critiques

- ▶ **logiciel**: texte relativement long écrit dans un langage spécifique et qui sera **exécuté par un ordinateur**
- ▶ **critique**: une défaillance peut avoir des **conséquences désastreuses** en termes humains ou économiques

Dans la vie quotidienne ...

Zune : le bug de l'an 2009 !



Il redémarre tout seul puis reste figé sur l'écran de démarrage.

Dans la vie quotidienne ... ou presque !

Sonde Mars Climate Orbiter - 26 septembre 1999



Perte de la sonde due ...

Dans la vie quotidienne ... ou presque !

Sonde Mars Climate Orbiter - 26 septembre 1999



Perte de la sonde due ... à un problème d'**unité de mesure** !

Équipe projet SECSI

Sécurité des Systèmes d'Information

- ▶ 4 permanents: H. Comon-Lundh, S. Delaune, J. Goubault-Larrecq, et G. Steel.



- ▶ 3 membres temporaires
- ▶ 4 doctorants

Protocoles cryptographiques



PayPal[™]

- ▶ petits programmes destinés à **sécuriser** nos communications (*e.g.* confidentialité, authentification)
- ▶ **omniprésents** dans notre vie quotidienne.

Protocoles cryptographiques



PayPalTM

- ▶ petits programmes destinés à **sécuriser** nos communications (e.g. confidentialité, authentification)
- ▶ **omniprésents** dans notre vie quotidienne.



Protocoles cryptographiques



PayPal™

- ▶ petits programmes destinés à **sécuriser** nos communications (e.g. confidentialité, authentification)
- ▶ **omniprésents** dans notre vie quotidienne.

Nos informations personnelles sont en danger !

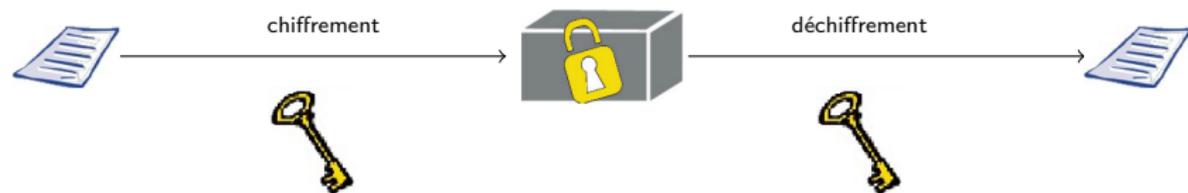




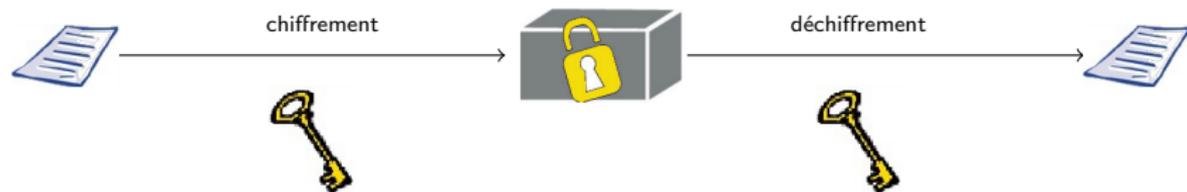
Le chiffrement

« HQVFD FKDQ »

Chiffrement symétrique



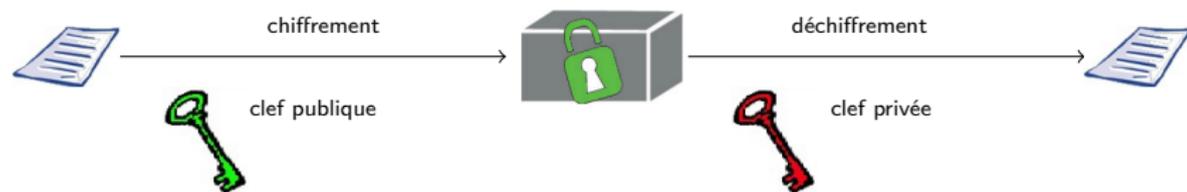
Chiffrement symétrique



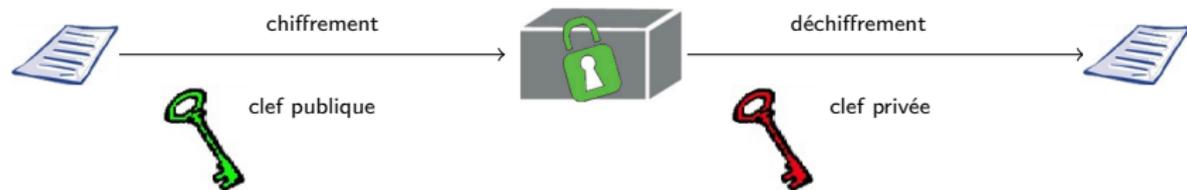
Quelques dates repères:

- ▶ 2000 avant J.-C.: traces de son utilisation par les Égyptiens
- ▶ 1920: machine Enigma
- ▶ 1977: Data Encryption Standard (DES)
- ▶ 2000: Advanced Encryption Standard (AES)

Chiffrement asymétrique (ou à clefs publiques)



Chiffrement asymétrique (ou à clefs publiques)



1977: chiffrement RSA (encore utilisé à l'heure actuelle)

- ▶ cette méthode de chiffrement repose sur un **problème mathématique** bien connu: **le problème de la factorisation**.

Chiffrement asymétrique (ou à clefs publiques)



1977: chiffrement RSA (encore utilisé à l'heure actuelle)

- ▶ cette méthode de chiffrement repose sur un **problème mathématique** bien connu: **le problème de la factorisation**.

Nombre à 96 chiffres

→ utilisé pour sécuriser les cartes bancaires dans les années 80 et 90.

213598703592091008239502270499962879705109534182
6417406442524165008583957746445088405009430865999



Mais chiffrer ne suffit pas toujours !



Le passeport électronique



Le vote électronique

La carte bancaire



Le smartphone



Vote électronique

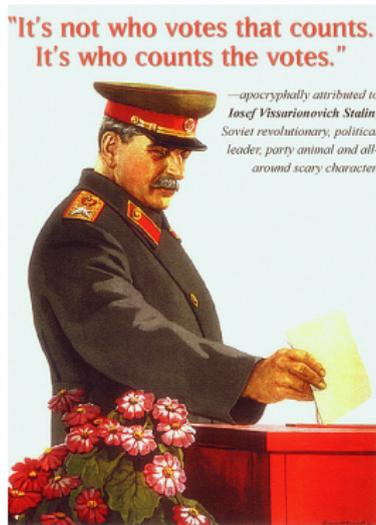


Vote électronique

La démocratie est-elle en péril ?

Avantages:

- ▶ **pratique**: différents types de scrutins, possibilité de voter de chez soi, ...
- ▶ **décompte efficace** des bulletins.



... mais il est souvent **opaque** et **invérifiable** !

Deux grandes familles



Machines à voter

- ▶ utilisation des bureaux de vote / isolement;
- ▶ mécanisme d'authentification externe (e.g. carte d'identité)

Deux grandes familles



Machines à voter

- ▶ utilisation des bureaux de vote / isolements;
- ▶ mécanisme d'authentification externe (e.g. carte d'identité)

→ utilisées dans 82 communes - élections présidentielles 2007

Deux grandes familles



Machines à voter

- ▶ utilisation des bureaux de vote / isolements;
- ▶ mécanisme d'authentification externe (e.g. carte d'identité)

→ utilisées dans 82 communes - élections présidentielles 2007

Vote par Internet

- ▶ possibilité de voter de chez soi avec son ordinateur personnel;



Deux grandes familles



Machines à voter

- ▶ utilisation des bureaux de vote / isolements;
- ▶ mécanisme d'authentification externe (e.g. carte d'identité)

→ utilisées dans 82 communes - élections présidentielles 2007

Vote par Internet

- ▶ possibilité de voter de chez soi avec son ordinateur personnel;

→ 11 députés à l'Assemblée nationale ont été élus par voie électronique - élections législatives juin 2012



Qu'est-ce qu'un bon protocole de vote ?

Équité

Vérifiabilité individuelle

Absence de reçu

Résistance à la coercition

Vérifiabilité universelle

Éligibilité

Anonymat

Qu'est-ce qu'un bon protocole de vote ?

Vérifiabilité individuelle

Équité

Absence de reçu **Résistance à la coercition**

Vérifiabilité universelle

Éligibilité

Anonymat

Est-ce qu'un bon protocole de vote existe ?

Qu'est-ce qu'un bon protocole de vote ?

Vérifiabilité individuelle

Équité

Absence de reçu **Résistance à la coercition**

Vérifiabilité universelle

Éligibilité

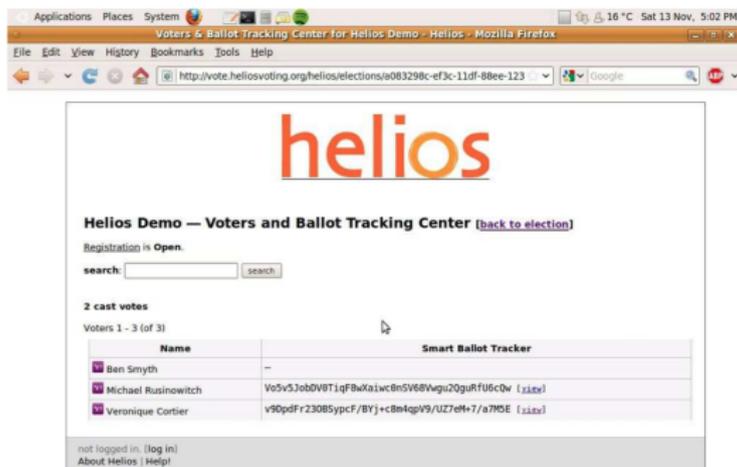
Anonymat

Est-ce qu'un bon protocole de vote existe ?

→ protocoles souvent **complexes**, utilisant des mécanismes cryptographiques « exotiques » et ne satisfaisant qu'un **sous-ensemble** des propriétés de sécurité ci-dessus.

Helios

→ développé par Ben Adida *et al.* (2009)



The screenshot shows a web browser window displaying the Helios interface. The browser's address bar shows the URL: `http://vote.heliosvoting.org/helios/elections/a083298c-ef3c-11d3-88ee-123`. The page title is "Voters & Ballot Tracking Center for Helios Demo - Helios - Mozilla Firefox". The main content area features the "helios" logo in orange and red. Below the logo, the text reads "Helios Demo — Voters and Ballot Tracking Center" with a link to "[back to election](#)". A status message says "Registration is Open." followed by a search bar with the label "search:" and a "search" button. Below this, it says "2 cast votes" and "Voters 1 - 3 (of 3)". A table lists the voters:

Name	Smart Ballot Tracker
Ben Smyth	-
Michael Rusinowitch	Vo5v5J0b0VBT1qf8wXaiwc8n5V68Vegu20guRfU6cQw
Veronique Cortier	v50pdFr23085ypcF/BYj+c8m4q/V9/UZ7ef+7/a7MSE

At the bottom of the page, there is a footer with the text "not logged in. (log in) About Helios | Help!"

→ utilisé lors de plusieurs élections: à l'UCL, à l'Université de Princeton, ...

Protocole Helios (version simplifiée)

Phase de vote: (valeur 0 ou 1)

Tableau d'affichage

<i>Alice</i>	$\{v_A\}_{\text{pub}(S)}$
<i>Bob</i>	$\{v_B\}_{\text{pub}(S)}$
<i>Chris</i>	$\{v_C\}_{\text{pub}(S)}$



Protocole Helios (version simplifiée)

Phase de vote: (valeur 0 ou 1)

Tableau d'affichage

Alice	$\{v_A\}_{\text{pub}(S)}$
Bob	$\{v_B\}_{\text{pub}(S)}$
Chris	$\{v_C\}_{\text{pub}(S)}$

$\{v_D\}_{\text{pub}(S)}$



Protocole Helios (version simplifiée)

Phase de vote: (valeur 0 ou 1)

Tableau d'affichage

<i>Alice</i>	$\{v_A\}_{\text{pub}(S)}$
<i>Bob</i>	$\{v_B\}_{\text{pub}(S)}$
<i>Chris</i>	$\{v_C\}_{\text{pub}(S)}$
<i>David</i>	$\{v_D\}_{\text{pub}(S)}$



Protocole Helios (version simplifiée)

Phase de vote: (valeur 0 ou 1)

Tableau d'affichage

Alice	$\{v_A\}_{\text{pub}(S)}$
Bob	$\{v_B\}_{\text{pub}(S)}$
Chris	$\{v_C\}_{\text{pub}(S)}$
David	$\{v_D\}_{\text{pub}(S)}$



Phase de comptage: utilisation du chiffrement homomorphe

$$\{v_A\}_{\text{pub}(S)} \times \{v_B\}_{\text{pub}(S)} \times \dots = \{v_A + v_B + \dots\}_{\text{pub}(S)}$$

→ Ainsi seul le résultat final sera déchiffré.

Protocole Helios (version simplifiée)

Phase de vote: (valeur 0 ou 1)

Tableau d'affichage

Alice	$\{v_A\}_{pub(S)}$
Bob	$\{v_B\}_{pub(S)}$
Chris	$\{v_C\}_{pub(S)}$
David	$\{v_D\}_{pub(S)}$



Phase de comptage: utilisation du chiffrement homomorphe

$$\{v_A\}_{pub(S)} \times \{v_B\}_{pub(S)} \times \dots = \{v_A + v_B + \dots\}_{pub(S)}$$

→ Ainsi seul le résultat final sera déchiffré.

Un votant malhonnête pourrait tricher !

Protocole Helios (version simplifiée)

Phase de vote: (valeur 0 ou 1)

Tableau d'affichage

Alice	$\{v_A\}_{\text{pub}(S)}$
Bob	$\{v_B\}_{\text{pub}(S)}$
Chris	$\{v_C\}_{\text{pub}(S)}$
David	$\{v_D\}_{\text{pub}(S)}$



Phase de comptage: utilisation du chiffrement homomorphe

$$\{v_A\}_{\text{pub}(S)} \times \{v_B\}_{\text{pub}(S)} \times \dots = \{v_A + v_B + \dots\}_{\text{pub}(S)}$$

→ Ainsi seul le résultat final sera déchiffré.

Un votant malhonnête pourrait tricher !

$\{v_D\}_{\text{pub}(S)}$ " + " preuve que v_D est égal à 0 ou 1

Protocole Helios

Vérifiabilité individuelle et universelle

Helios satisfait a priori les différentes formes de **vérifiabilité**.

Protocole Helios

Vérifiabilité individuelle et universelle

Helios satisfait a priori les différentes formes de **vérifiabilité**.

Anonymat, sans reçu, et résistance à la coercition

- ▶ Helios ne résiste pas aux formes de coercition les plus fortes
→ il est possible d'obtenir un reçu de son vote

Protocole Helios

Vérifiabilité individuelle et universelle

Helios satisfait a priori les différentes formes de **vérifiabilité**.

Anonymat, sans reçu, et résistance à la coercition

- ▶ Helios ne résiste pas aux formes de coercition les plus fortes
→ il est possible d'obtenir un reçu de son vote
- ▶ **Helios ne satisfait même pas l'anonymat !**
→ il est possible de rejouer un message et de voter comme une autre votant de son choix (sans pour autant connaître la valeur de son vote)

Attaque découverte en 2011 par B. Smyth et V. Cortier

Comment vérifier ces protocoles ?

Les mathématiques et l'informatique à la rescousse !

Comment vérifier ces protocoles ?

Les mathématiques et l'informatique à la rescousse !

Notre but:

1. faire des preuves mathématiques rigoureuses,
2. d'une façon automatique.

« Construire une machine à détecter les bugs »

Comment vérifier ces protocoles ?

Les mathématiques et l'informatique à la rescousse !

Notre but:

1. faire des preuves mathématiques rigoureuses,
2. d'une façon automatique.

« Construire une machine à détecter les bugs »

1936: une telle machine n'existe pas (Alan Turing)

... même dans le cas particulier des protocoles cryptographiques.



Mais alors, que faisons-nous ?

Le problème n'a **pas de solution**

Mais alors, que faisons-nous ?

Le problème n'a **pas de solution**
mais seulement dans le **cas général**



Mais alors, que faisons-nous ?

Le problème n'a **pas de solution**
mais seulement dans le **cas général**



Différentes pistes:

- ▶ résoudre le problème dans de nombreux **cas intéressants**
- ▶ proposer des **procédures approchées**

Mais alors, que faisons-nous ?

Le problème n'a **pas de solution**
mais seulement dans le **cas général**



Différentes pistes:

- ▶ résoudre le problème dans de nombreux **cas intéressants**
- ▶ proposer des **procédures approchées**

→ **Prix Turing** décerné à JOSEPH SIFAKIS en 2007 pour ses travaux sur le model-checking.

Outil de vérification AVISPA

Outil disponible en ligne: <http://www.avispa-project.org/>

The screenshot displays the AVISPA web tool interface. The main window is titled "AVISPA Automated Verification of Internet Security Protocols and Applications". It features a "Protocol" section with a list of protocols, including "SPM" (Secure Protocol Mechanism). Below this, there is a "Tools" section with buttons for "AVISPA", "AVISPA", and "AVISPA". The "AVISPA" button is highlighted. The interface also shows a "Tools" section with buttons for "AVISPA", "AVISPA", and "AVISPA".

On the right side, there is a "Code" window showing the protocol definition in AVISPA syntax. The code includes a "state" block with variables like "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", "aa", "ab", "ac", "ad", "ae", "af", "ag", "ah", "ai", "aj", "ak", "al", "am", "an", "ao", "ap", "aq", "ar", "as", "at", "au", "av", "aw", "ax", "ay", "az", "ba", "bb", "bc", "bd", "be", "bf", "bg", "bh", "bi", "bj", "bk", "bl", "bm", "bn", "bo", "bp", "bq", "br", "bs", "bt", "bu", "bv", "bw", "bx", "by", "bz", "ca", "cb", "cc", "cd", "ce", "cf", "cg", "ch", "ci", "cj", "ck", "cl", "cm", "cn", "co", "cp", "cq", "cr", "cs", "ct", "cu", "cv", "cw", "cx", "cy", "cz", "da", "db", "dc", "dd", "de", "df", "dg", "dh", "di", "dj", "dk", "dl", "dm", "dn", "do", "dp", "dq", "dr", "ds", "dt", "du", "dv", "dw", "dx", "dy", "dz", "ea", "eb", "ec", "ed", "ee", "ef", "eg", "eh", "ei", "ej", "ek", "el", "em", "en", "eo", "ep", "eq", "er", "es", "et", "eu", "ev", "ew", "ex", "ey", "ez", "fa", "fb", "fc", "fd", "fe", "ff", "fg", "fh", "fi", "fj", "fk", "fl", "fm", "fn", "fo", "fp", "fq", "fr", "fs", "ft", "fu", "fv", "fw", "fx", "fy", "fz", "ga", "gb", "gc", "gd", "ge", "gf", "gg", "gh", "gi", "gj", "gk", "gl", "gm", "gn", "go", "gp", "gq", "gr", "gs", "gt", "gu", "gv", "gw", "gx", "gy", "gz", "ha", "hb", "hc", "hd", "he", "hf", "hg", "hh", "hi", "hj", "hk", "hl", "hm", "hn", "ho", "hp", "hq", "hr", "hs", "ht", "hu", "hv", "hw", "hx", "hy", "hz", "ia", "ib", "ic", "id", "ie", "if", "ig", "ih", "ii", "ij", "ik", "il", "im", "in", "io", "ip", "iq", "ir", "is", "it", "iu", "iv", "iw", "ix", "iy", "iz", "ja", "jb", "jc", "jd", "je", "jf", "jg", "jh", "ji", "jj", "jk", "jl", "jm", "jn", "jo", "jp", "jq", "jr", "js", "jt", "ju", "jv", "jw", "jx", "jy", "jz", "ka", "kb", "kc", "kd", "ke", "kf", "kg", "kh", "ki", "kj", "kk", "kl", "km", "kn", "ko", "kp", "kq", "kr", "ks", "kt", "ku", "kv", "kw", "kx", "ky", "kz", "la", "lb", "lc", "ld", "le", "lf", "lg", "lh", "li", "lj", "lk", "ll", "lm", "ln", "lo", "lp", "lq", "lr", "ls", "lt", "lu", "lv", "lw", "lx", "ly", "lz", "ma", "mb", "mc", "md", "me", "mf", "mg", "mh", "mi", "mj", "mk", "ml", "mn", "mo", "mp", "mq", "mr", "ms", "mt", "mu", "mv", "mw", "mx", "my", "mz", "na", "nb", "nc", "nd", "ne", "nf", "ng", "nh", "ni", "nj", "nk", "nl", "nm", "no", "np", "nq", "nr", "ns", "nt", "nu", "nv", "nw", "nx", "ny", "nz", "oa", "ob", "oc", "od", "oe", "of", "og", "oh", "oi", "oj", "ok", "ol", "om", "on", "oo", "op", "oq", "or", "os", "ot", "ou", "ov", "ow", "ox", "oy", "oz", "pa", "pb", "pc", "pd", "pe", "pf", "pg", "ph", "pi", "pj", "pk", "pl", "pm", "pn", "po", "pp", "pq", "pr", "ps", "pt", "pu", "pv", "pw", "px", "py", "pz", "qa", "qb", "qc", "qd", "qe", "qf", "qg", "qh", "qi", "qj", "qk", "ql", "qm", "qn", "qo", "qp", "qq", "qr", "qs", "qt", "qu", "qv", "qw", "qx", "qy", "qz", "ra", "rb", "rc", "rd", "re", "rf", "rg", "rh", "ri", "rj", "rk", "rl", "rm", "rn", "ro", "rp", "rq", "rr", "rs", "rt", "ru", "rv", "rw", "rx", "ry", "rz", "sa", "sb", "sc", "sd", "se", "sf", "sg", "sh", "si", "sj", "sk", "sl", "sm", "sn", "so", "sp", "sq", "sr", "ss", "st", "su", "sv", "sw", "sx", "sy", "sz", "ta", "tb", "tc", "td", "te", "tf", "tg", "th", "ti", "tj", "tk", "tl", "tm", "tn", "to", "tp", "tq", "tr", "ts", "tt", "tu", "tv", "tw", "tx", "ty", "tz", "ua", "ub", "uc", "ud", "ue", "uf", "ug", "uh", "ui", "uj", "uk", "ul", "um", "un", "uo", "up", "uq", "ur", "us", "ut", "uu", "uv", "uw", "ux", "uy", "uz", "va", "vb", "vc", "vd", "ve", "vf", "vg", "vh", "vi", "vj", "vk", "vl", "vm", "vn", "vo", "vp", "vq", "vr", "vs", "vt", "vu", "vv", "vw", "vx", "vy", "vz", "wa", "wb", "wc", "wd", "we", "wf", "wg", "wh", "wi", "wj", "wk", "wl", "wm", "wn", "wo", "wp", "wq", "wr", "ws", "wt", "wu", "wv", "ww", "wx", "wy", "wz", "xa", "xb", "xc", "xd", "xe", "xf", "xg", "xh", "xi", "xj", "xk", "xl", "xm", "xn", "xo", "xp", "xq", "xr", "xs", "xt", "xu", "xv", "xw", "xx", "xy", "xz", "ya", "yb", "yc", "yd", "ye", "yf", "yg", "yh", "yi", "yj", "yk", "yl", "ym", "yn", "yo", "yp", "yq", "yr", "ys", "yt", "yu", "yv", "yw", "yx", "yy", "yz", "za", "zb", "zc", "zd", "ze", "zf", "zg", "zh", "zi", "zj", "zk", "zl", "zm", "zn", "zo", "zp", "zq", "zr", "zs", "zt", "zu", "zv", "zw", "zx", "zy", "zz".

Below the code, there is an "Attack Trace" section showing a sequence of messages between three agents (Agent 1, Agent 2, Agent 3). The messages are represented as boxes with labels like "a.b.m", "c.d.n", "e.f.o", "g.h.p", "i.j.q", "k.l.r", "m.n.s", "o.p.t", "q.r.u", "s.t.v", "u.v.w", "x.y.z", "aa.bb", "cc.dd", "ee.ff", "gg.hh", "ii.jj", "kk.ll", "mm.nn", "oo.pp", "qq.rr", "ss.tt", "uu.vv", "ww.xx", "yy.zz".

→ Projet Européen (France, Italie, Allemagne, Suisse)

Conclusion

Les **méthodes formelles** permettent une bonne analyse des protocoles cryptographiques.

- ▶ découverte de failles à l'aide d'outil de vérification;
- ▶ des **preuves formelles** de sécurité peuvent être obtenues automatiquement (sans intervention humaine).

Conclusion

Les **méthodes formelles** permettent une bonne analyse des protocoles cryptographiques.

- ▶ découverte de failles à l'aide d'outil de vérification;
- ▶ des **preuves formelles** de sécurité peuvent être obtenues automatiquement (sans intervention humaine).

Il reste cependant beaucoup à faire:

- ▶ savoir analyser différentes **propriétés de sécurité**
→ l'**anonymat** sous toutes ses formes!
- ▶ prendre en compte les **propriétés mathématiques** du chiffrement (e.g. chiffrement homomorphique)
- ▶ réaliser ses analyses formelles dans des modèles plus réalistes.

MERCI