Les mathématiques de la cryptologie, I

Jean-Marc Couveignes

Université de Bordeaux

Lycée François Magendie, Bordeaux

Fonctionalités cryptographiques

à quoi sert la cryptographie ?

Fonctionalités cryptographiques

à quoi sert la cryptographie ?

- Chiffrement (pli confidentiel)

Fonctionalités cryptographiques

à quoi sert la cryptographie ?

- Chiffrement (pli confidentiel)
- Identification (badge cantine, carte à puce, empreinte digitale)

Fonctionalités cryptographiques

à quoi sert la cryptographie ?

- Chiffrement (pli confidentiel)
- Identification (badge cantine, carte à puce, empreinte digitale)
- Intégrité (clé RIB, scellés)

Fonctionalités cryptographiques

à quoi sert la cryptographie ?

- Chiffrement (pli confidentiel)
- Identification (badge cantine, carte à puce, empreinte digitale)
- Intégrité (clé RIB, scellés)
- Signature (ordre de virement) : identification, intégrité, non-répudiation

Fonctionalités cryptographiques

à quoi sert la cryptographie ?

- Chiffrement (pli confidentiel)
- Identification (badge cantine, carte à puce, empreinte digitale)
- Intégrité (clé RIB, scellés)
- Signature (ordre de virement) : identification, intégrité, non-répudiation
- Vie privée, anonymat, argent électronique

Fonctionalités cryptographiques

à quoi sert la cryptographie ?

- Chiffrement (pli confidentiel)
- Identification (badge cantine, carte à puce, empreinte digitale)
- Intégrité (clé RIB, scellés)
- Signature (ordre de virement) : identification, intégrité, non-répudiation
- Vie privée, anonymat, argent électronique
- ...

Chiffrement

Alice 

Chiffrement

Alice 

veut écrire

Chiffrement

Alice 

veut écrire

à Bob 

Chiffrement de Jules César

Alice 

Chiffrement de Jules César

Alice 

QUARTIQUE

Chiffrement de Jules César

Alice

QUARTIQUE

clé de chiffrement +3

Chiffrement de Jules César

Alice

QUARTIQUE

clé de chiffrement +3

TXDUWLTXH

Chiffrement de Jules César

Alice

QUARTIQUE

clé de chiffrement +3

TXDUWLTXH

TXDUWLTXH est envoyé

Chiffrement de Jules César

Alice 

QUARTIQUE

clé de chiffrement +3

TXDUWLTXH

TXDUWLTXH est envoyé

à Bob 

Chiffrement de Jules César

Alice

QUARTIQUE

clé de chiffrement +3

TXDUWLTXH

TXDUWLTXH est envoyé

à Bob

TXDUWLTXH

Chiffrement de Jules César

Alice

QUARTIQUE

clé de chiffrement +3

TXDUWLTXH

TXDUWLTXH est envoyé

à Bob

TXDUWLTXH

clé de déchiffrement -3

Chiffrement de Jules César

Alice

QUARTIQUE

clé de chiffrement +3

TXDUWLTXH

TXDUWLTXH est envoyé

à Bob

TXDUWLTXH

clé de déchiffrement -3 QUARTIQUE

Chiffrement à clé secrète

Alice 

Chiffrement à clé secrète

Alice 

m=QUARTIQUE

Chiffrement à clé secrète

Alice 

m=QUARTIQUE

clé secrète de chiffrement $K = +3$

Chiffrement à clé secrète

Alice 

m=QUARTIQUE

clé secrète de chiffrement $K = +3$

$c = f_K(m)$

Chiffrement à clé secrète

Alice 

m=QUARTIQUE

clé secrète de chiffrement $K = +3$

$c = f_K(m)$

c =TXDUWLTXH est envoyé

Chiffrement à clé secrète

Alice 

m=QUARTIQUE

clé secrète de chiffrement $K = +3$

$c = f_K(m)$

c =TXDUWLTXH est envoyé

à Bob 

Chiffrement à clé secrète

Alice 

m=QUARTIQUE

clé secrète de chiffrement $K = +3$

$c = f_K(m)$

c =TXDUWLTXH est envoyé

à Bob 

c =TXDUWLTXH

Chiffrement à clé secrète

Alice 

m=QUARTIQUE

clé secrète de chiffrement $K = +3$

$c = f_K(m)$

c =TXDUWLTXH est envoyé

à Bob 

c =TXDUWLTXH

clé secrète de déchiffrement $K' = -K = -3$

Chiffrement à clé secrète

Alice

m=QUARTIQUE

clé secrète de chiffrement $K = +3$

$c = f_K(m)$

c =TXDUWLTXH est envoyé

à Bob

c =TXDUWLTXH

clé secrète de déchiffrement $K' = -K = -3$

$m = f_K{}^{(-1)}(c) = f_{K'}(c)$

Un exemple

Chiffrer le message m=TRAVAUX avec la méthode de Jules César et la clé de chiffrement K=+7.

Un exemple

Chiffrer le message m=TRAVAUX avec la méthode de Jules César et la clé de chiffrement K=+7.

c = AYHCHBE

Un exemple

Chiffrer le message m=TRAVAUX avec la méthode de Jules César et la clé de chiffrement K=+7.

c = AYHCHBE

Déchiffrer le chiffré c=IVUQVBY en supposant qu'il a été chiffré avec la méthode de Jules César et la clé de chiffrement K=+7.

Un exemple

Chiffrer le message m=TRAVAUX avec la méthode de Jules César et la clé de chiffrement K=+7.

c = AYHCHBE

Déchiffrer le chiffré c=IVUQVBY en supposant qu'il a été chiffré avec la méthode de Jules César et la clé de chiffrement K=+7.

m=BONJOUR

Un exemple

Chiffrer le message m=TRAVAUX avec la méthode de Jules César et la clé de chiffrement K=+7.

c = AYHCHBE

Déchiffrer le chiffré c=IVUQVBY en supposant qu'il a été chiffré avec la méthode de Jules César et la clé de chiffrement K=+7.

m=BONJOUR

Le chiffré FHGLBXNK a été chiffré avec la méthode de Jules César.
On sait que la première lettre du clair est un M.
Quelle est la clé ?
Quel est le clair ?

Un exemple

Chiffrer le message m=TRAVAUX avec la méthode de Jules César et la clé de chiffrement K=+7.

c = AYHCHBE

Déchiffrer le chiffré c=IVUQVBY en supposant qu'il a été chiffré avec la méthode de Jules César et la clé de chiffrement K=+7.

m=BONJOUR

Le chiffré FHGLBXNK a été chiffré avec la méthode de Jules César.
On sait que la première lettre du clair est un M.
Quelle est la clé ?
Quel est le clair ?

m=MONSIEUR et K=19

Chiffrement à clé secrète

- Trois étapes : création et distribution de clés, chiffrement, déchiffrement
- Boîte mail, consultation de compte en banque, ...
- Avantages : simple, rapide, bien connu
- Complexe : gestion de clés
- Fragilités : attaque exhaustive, autres attaques,

L'attaque exhaustive

On note $26! = 1 \times 2 \times 3 \times \cdots \times 24 \times 25 \times 26$.

L'attaque exhaustive

On note $26! = 1 \times 2 \times 3 \times \cdots \times 24 \times 25 \times 26$.

C'est le nombre de substitutions avec un alphabet de 26 lettres.

L'attaque exhaustive

On note $26! = 1 \times 2 \times 3 \times \cdots \times 24 \times 25 \times 26$.

C'est le nombre de substitutions avec un alphabet de 26 lettres.

Vérifiez avec votre calculette que 26! est dans l'intervalle $[4 \times 10^{26}, 5 \times 10^{26}]$.

L'attaque exhaustive

On note $26! = 1 \times 2 \times 3 \times \cdots \times 24 \times 25 \times 26$.

C'est le nombre de substitutions avec un alphabet de 26 lettres.

Vérifiez avec votre calculette que 26! est dans l'intervalle $[4 \times 10^{26}, 5 \times 10^{26}]$.
On suppose qu'un processeur peut essayer un milliard de clés par seconde.
Montrer qu'il lui faudra au moins dix milliards d'années pour les essayer toutes.

Attaque statistique : qui est l'espace ?

qmtzrmboltshtzwcobwqltslvtzwccmkvvmczlvtvtmppqkihltmhntsk
pqwjlvtcmokwcmhntsltqkzlczltlotjmvolbtlotmhntskpqwjlvtkco
lbjlskmkblvtsltslhytlotjmkobkvltslqkablvtpmbtqthckalbvkol

t 26, l 24, k 14, m 13, v 12

Attaque statistique : qui est l'espace ?

qmtzrmboltshtzwcobwqltslvtzwccmkvvmczlvtvtmppqkihltmhntsk
pqwjlvtcmokwcmhntsltqkzlczltlotjmvolbtlotmhntskpqwjlvtkco
lbjlskmkblvtsltslhytlotjmkobkvltslqkablvtpmbtqthckalbvkol

t 26, l 24, k 14, m 13, v 12

qm zrmbol sh zwcobwql slv zwccmkvvmczlv v mppqkihl mhn sk
pqwjlv cmokwcmhn sl qkzlczl lo jmvolb lo mhn skpqwjlv kco
lbjlskmkblv sl slhy lo jmkobkvl slqkablv pmb q hckalbvkol

Attaque statistique : qui est l'espace ?

qmtzrmboltshtzwcobwqltslvtzwccmkvvmczlvtvtmppqkihltmhntsk
pqwjlvtcmokwcmhntsltqkzlczltlotjmvolbtlotmhntskpqwjlvtkco
lbjlskmkblvtsltslhytlotjmkobkvltslqkablvtpmbtqthckalbvkol

t 26, l 24, k 14, m 13, v 12

qm zrmbol sh zwcobwql slv zwccmkvvmczlv v mppqkihl mhn sk
pqwjlv cmokwcmhn sl qkzlczl lo jmvolb lo mhn skpqwjlv kco
lbjlskmkblv sl slhy lo jmkobkvl slqkablv pmb q hckalbvkol

qmtzrmbo tshtzwcobwq ts vtzwccmkvvmcz vtvtmppqkih tmhntsk
pqwj vtcmokwcmhnts tqkz cz t otjmvo bt otmhntskpqwj vtkco bj
skmkb vts ts hyt otjmkobkv ts qkab vtpmbtqthcka bvko

Attaque statistique : qui est l'espace ?

qmtzrmboltshtzwcobwqltslvtzwccmkvvmczlvtvtmppqkihltmhntsk
pqwjlvtcmokwcmhntsltqkzlczltlotjmvolbtlotmhntskpqwjlvtkco
lbjlskmkblvtsltslhytlotjmkobkvltslqkablvtpmbtqthckalbvkol

t 26, l 24, k 14, m 13, v 12

qm zrmbol sh zwcobwql slv zwccmkvvmczlv v mppqkihl mhn sk
pqwjlv cmokwcmhn sl qkzlczl lo jmvolb lo mhn skpqwjlv kco
lbjlskmkblv sl slhy lo jmkobkvl slqkablv pmb q hckalbvkol

qmtzrmbo tshtzwcobwq ts vtzwccmkvvmcz vtvtmppqkih tmhntsk
pqwj vtcmokwcmhnts tqkz cz t otjmvo bt otmhntskpqwj vtkco bj
skmkb vts ts hyt otjmkobkv ts qkab vtpmbtqthcka bvko

qmtzrmboltshtzwcobwqltslvtzwccm vvmczlvtvtmppq ihltmhnts
pqwjlvtcmo wcmhntsltq zlczltlotjmvolbtlotmhnts pqwjlvt co lbjls m
blvtsltslhytlotjm ob vltslq ablvtpmbtqthc albv ol

Attaque statistique : qui est E

qm zrmbol sh zwcobwql slv zwccmkvvmczlv v mppqkihl mhn sk pqwjlv cmokwcmhn sl qkzlczl lo jmvolb lo mhn skpqwjlv kco lbjlskmkblv sl slhy lo jmkobkvl slqkablv pmb q hckalbvkol

Attaque statistique : qui est E

qm zrmbol sh zwcobwql slv zwccmkvvmczlv v mppqkihl mhn sk pqwjlv cmokwcmhn sl qkzlczl lo jmvolb lo mhn skpqwjlv kco lbjlskmkblv sl slhy lo jmkobkvl slqkablv pmb q hckalbvkol

l 24, k 14, m 13, v 12

Attaque statistique : qui est E

qm zrmbol sh zwcobwql slv zwccmkvvmczlv v mppqkihl mhn sk pqwjlv cmokwcmhn sl qkzlczl lo jmvolb lo mhn skpqwjlv kco lbjlskmkblv sl slhy lo jmkobkvl slqkablv pmb q hckalbvkol

l 24, k 14, m 13, v 12

l est E

Attaque statistique : qui est E

qm zrmbol sh zwcobwql slv zwccmkvvmczlv v mppqkihl mhn sk pqwjlv cmokwcmhn sl qkzlczl lo jmvolb lo mhn skpqwjlv kco lbjlskmkblv sl slhy lo jmkobkvl slqkablv pmb q hckalbvkol

l 24, k 14, m 13, v 12

l est E
qm zrmboE sh zwcobwqE sEv zwccmkvvmczEv v mppqkihE mhn sk pqwjEv cmokwcmhn sE qkzEczE Eo jmvoEb Eo mhn skpqwjEv kco EbjEskmkbEv sE sEhy Eo jmkobkvE sEqkabEv pmb q hckaEbvkoE

Attaque statistique : qui est v

qm zrmboE sh zwcobwqE sEv zwccmkvvmczEv v mppqkihE mhn sk pqwjEv cmokwcmhn sE qkzEczE Eo jmvoEb Eo mhn skpqwjEv kco EbjEskmkbEv sE sEhy Eo jmkobkvE sEqkabEv pmb q hckaEbvkoE

Attaque statistique : qui est v

qm zrmboE sh zwcobwqE sEv zwccmkvvmczEv v mppqkihE mhn sk pqwjEv cmokwcmhn sE qkzEczE Eo jmvoEb Eo mhn skpqwjEv kco EbjEskmkbEv sE sEhy Eo jmkobkvE sEqkabEv pmb q hckaEbvkoE

les v à la fin des mots sont des S

Attaque statistique : qui est v

qm zrmboE sh zwcobwqE sEv zwccmkvvmczEv v mppqkihE mhn sk pqwjEv cmokwcmhn sE qkzEczE Eo jmvoEb Eo mhn skpqwjEv kco EbjEskmkbEv sE sEhy Eo jmkobkvE sEqkabEv pmb q hckaEbvkoE

les v à la fin des mots sont des S

qm zrmboE sh zwcobwqE sES zwccmkSSmczES S mppqkihE mhn sk pqwjES cmokwcmhn sE qkzEczE Eo jmSoEb Eo mhn skpqwjES kco EbjEskmkbES sE sEhy Eo jmkobkSE sEqkabES pmb q hckaEbSkoE

Attaque statistique : qui est A ?

t 26 -> espace
l 24 ->E
k 14
m 13
v 12 ->S

Attaque statistique : qui est A ?

t 26 -> espace
l 24 ->E
k 14
m 13
v 12 ->S

Le A est k ou m.

qm zrmboE sh zwcobwqE sES zwccmkSSmczES S mppqkihE mhn sk pqwjES cmokwcmhn sE qkzEczE Eo jmSoEb Eo mhn skpqwjES kco EbjEskmkbES sE sEhy Eo jmkobkSE sEqkabES pmb q hckaEbSkoE

Attaque statistique : qui est A ?

t 26 -> espace
l 24 ->E
k 14
m 13
v 12 ->S

Le A est k ou m.

qm zrmboE sh zwcobwqE sES zwccmkSSmczES S mppqkihE mhn sk pqwjES cmokwcmhn sE qkzEczE Eo jmSoEb Eo mhn skpqwjES kco EbjEskmkbES sE sEhy Eo jmkobkSE sEqkabES pmb q hckaEbSkoE

qm -> LA

Attaque statistique : qui est A ?

t 26 -> espace
l 24 ->E
k 14
m 13
v 12 ->S

Le A est k ou m.

qm zrmboE sh zwcobwqE sES zwccmkSSmczES S mppqkihE mhn sk pqwjES cmokwcmhn sE qkzEczE Eo jmSoEb Eo mhn skpqwjES kco EbjEskmkbES sE sEhy Eo jmkobkSE sEqkabES pmb q hckaEbSkoE

qm -> LA
LA zrAboE sh zwcobwLE sES zwccAkSSAczES S AppLkihE Ahn sk pLwjES cAokwcAhn sE LkzEczE Eo jASoEb Eo Ahn skpLwjES kco EbjEskAkbES sE sEhy Eo jAkobkSE sELkabES pAb L hckaEbSkoE

Attaque statistique : qui est k ?

t 26 ->esp
l 24 ->E
k 14
m 13 ->A
v 12 ->S

LA zrAboE sh zwcobwLE sES zwccAkSSAczES S AppLkihE Ahn sk pLwjES cAokwcAhn sE LkzEczE Eo jASoEb Eo Ahn skpLwjES kco EbjEskAkbES sE sEhy Eo jAkobkSE sELkabES pAb L hckaEbSkoE

Plutôt une voyelle.
La voyelle la plus fréquente après E et A est I.

Attaque statistique : qui est k ?

t 26 ->esp
l 24 ->E
k 14
m 13 ->A
v 12 ->S

LA zrAboE sh zwcobwLE sES zwccAkSSAczES S AppLkihE Ahn sk pLwjES cAokwcAhn sE LkzEczE Eo jASoEb Eo Ahn skpLwjES kco EbjEskAkbES sE sEhy Eo jAkobkSE sELkabES pAb L hckaEbSkoE

Plutôt une voyelle.
La voyelle la plus fréquente après E et A est I.

Donc on essaye k->I

Attaque statistique : qui est k ?

t 26 ->esp
l 24 ->E
k 14
m 13 ->A
v 12 ->S

LA zrAboE sh zwcobwLE sES zwccAkSSAczES S AppLkihE Ahn sk pLwjES cAokwcAhn sE LkzEczE Eo jASoEb Eo Ahn skpLwjES kco EbjEskAkbES sE sEhy Eo jAkobkSE sELkabES pAb L hckaEbSkoE

Plutôt une voyelle.
La voyelle la plus fréquente après E et A est I.

Donc on essaye k->I

LA zrAboE sh zwcobwLE sES zwccAISSAczES S AppLIihE Ahn sI pLwjES cAoIwcAhn sE LIzEczE Eo jASoEb Eo Ahn sIpLwjES Ico EbjEsIAIbES sE sEhy Eo jAIobISE sELIabES pAb L hcIaEbSIoE

Attaque statistique : que signifie zwccAkSSAczES

LA zrAboE sh zwcobwLE sES zwccAISSAczES S AppLIihE Ahn sI pLwjES cAoIwcAhn sE LIzEczE Eo jASoEb Eo Ahn sIpLwjES Ico EbjEsIAIbES sE sEhy Eo jAIobISE sELIabES pAb L hcIaEbSIoE

zwccAkSSAczES

Attaque statistique : que signifie zwccAkSSAczES

LA zrAboE sh zwcobwLE sES zwccAISSAczES S AppLIihE Ahn sI pLwjES cAoIwcAhn sE LIzEczE Eo jASoEb Eo Ahn sIpLwjES Ico EbjEsIAIbES sE sEhy Eo jAIobISE sELIabES pAb L hcIaEbSIoE

zwccAkSSAczES
****A*SSA**ES

Attaque statistique : que signifie zwccAkSSAczES

LA zrAboE sh zwcobwLE sES zwccAISSAczES S AppLIihE Ahn sI pLwjES cAoIwcAhn sE LIzEczE Eo jASoEb Eo Ahn sIpLwjES Ico EbjEsIAIbES sE sEhy Eo jAIobISE sELIabES pAb L hcIaEbSIoE

zwccAkSSAczES
****A*SSA**ES
CONNAISSANCES

Attaque statistique : que signifie zwccAkSSAczES

LA zrAboE sh zwcobwLE sES zwccAISSAczES S AppLIihE Ahn sI pLwjES cAoIwcAhn sE LIzEczE Eo jASoEb Eo Ahn sIpLwjES Ico EbjEsIAIbES sE sEhy Eo jAIobISE sELIabES pAb L hcIaEbSIoE

zwccAkSSAczES
****A*SSA**ES
CONNAISSANCES
z->C
w->O
c->N

Attaque statistique : que signifie zwccAkSSAczES

LA zrAboE sh zwcobwLE sES zwccAISSAczES S AppLIihE Ahn sI pLwjES cAoIwcAhn sE LIzEczE Eo jASoEb Eo Ahn sIpLwjES Ico EbjEsIAIbES sE sEhy Eo jAIobISE sELIabES pAb L hcIaEbSIoE

zwccAkSSAczES
****A*SSA**ES
CONNAISSANCES
z->C
w->O
c->N

LA CrAboE sh CONobOLE sES CONNAISSANCES S AppLIihE Ahn sI pLOjES NAoIONAhn sE LICENCE Eo jASoEb Eo Ahn sIpLOjES INo EbjEsIAIbES sE sEhy Eo jAIobISE sELIabES pAb L hNIaEbSIoE

Attaque statistique : que signifie NAoIONAhn

LA CrAboE sh CONobOLE sES CONNAISSANCES S AppLIihE Ahn sI pLOjES NAoIONAhn sE LICENCE Eo jASoEb Eo Ahn sIpLOjES INo EbjEsIAIbES sE sEhy Eo jAIobISE sELIabES pAb L hNIaEbSIoE

NAoIONAhn

Attaque statistique : que signifie NAoIONAhn

LA CrAboE sh CONobOLE sES CONNAISSANCES S AppLIihE Ahn sI pLOjES NAoIONAhn sE LICENCE Eo jASoEb Eo Ahn sIpLOjES INo EbjEsIAIbES sE sEhy Eo jAIobISE sELIabES pAb L hNIaEbSIoE

NAoIONAhn
NA*IONA**

Attaque statistique : que signifie NAoIONAhn

LA CrAboE sh CONobOLE sES CONNAISSANCES S AppLIihE Ahn sI pLOjES NAoIONAhn sE LICENCE Eo jASoEb Eo Ahn sIpLOjES INo EbjEsIAIbES sE sEhy Eo jAIobISE sELIabES pAb L hNIaEbSIoE

NAoIONAhn
NA*IONA**
NATIONAUX

Attaque statistique : que signifie NAoIONAhn

LA CrAboE sh CONobOLE sES CONNAISSANCES S AppLIihE Ahn sI pLOjES NAoIONAhn sE LICENCE Eo jASoEb Eo Ahn sIpLOjES INo EbjEsIAIbES sE sEhy Eo jAIobISE sELIabES pAb L hNIaEbSIoE

NAoIONAhn
NA*IONA**
NATIONAUX
o->T
h->U
n->X

Attaque statistique : que signifie NAoIONAhn

LA CrAboE sh CONobOLE sES CONNAISSANCES S AppLIihE Ahn sI pLOjES NAoIONAhn sE LICENCE Eo jASoEb Eo Ahn sIpLOjES INo EbjEsIAIbES sE sEhy Eo jAIobISE sELIabES pAb L hNIaEbSIoE

NAoIONAhn
NA*IONA**
NATIONAUX
o->T
h->U
n->X

LA CrAbTE sU CONTbOLE sES CONNAISSANCES S AppLIiUE AUX sI pLOjES NATIONAUX sE LICENCE ET jASTEb ET AUX sIpLOjES INT EbjEsIAIbES sE sEUy ET jAITbISE sELIabES pAb L UNIaEbSITE

Attaque statistique : que signifie NAoIONAhn

LA CrAbTE sU CONTbOLE sES CONNAISSANCES S AppLIiUE AUX sl pLOjES NATIONAUX sE LICENCE ET jASTEb ET AUX slpLOjES INT EbjEslAlbES sE sEUy ET jAITblSE sELIabES pAb L UNIaEbSITE

Attaque statistique : que signifie NAoIONAhn

LA CrAbTE sU CONTbOLE sES CONNAISSANCES S AppLIiUE AUX sl pLOjES NATIONAUX sE LICENCE ET jASTEb ET AUX slpLOjES INT EbjEslAlbES sE sEUy ET jAITblSE sELIabES pAb L UNIaEbSITE

CONTbOLE

Attaque statistique : que signifie NAoIONAhn

LA CrAbTE sU CONTbOLE sES CONNAISSANCES S AppLIiUE AUX sl pLOjES NATIONAUX sE LICENCE ET jASTEb ET AUX slpLOjES INT EbjEslAlbES sE sEUy ET jAITblSE sELIabES pAb L UNIaEbSITE

CONTbOLE CONT*OLE

Attaque statistique : que signifie NAoIONAhn

LA CrAbTE sU CONTbOLE sES CONNAISSANCES S AppLIiUE AUX sl pLOjES NATIONAUX sE LICENCE ET jASTEb ET AUX slpLOjES INT EbjEslAlbES sE sEUy ET jAITblSE sELIabES pAb L UNIaEbSITE

CONTbOLE CONT*OLE CONTROLE

Attaque statistique : que signifie NAoIONAhn

LA CrAbTE sU CONTbOLE sES CONNAISSANCES S AppLIiUE AUX sl pLOjES NATIONAUX sE LICENCE ET jASTEb ET AUX slpLOjES INT EbjEslAlbES sE sEUy ET jAITblSE sELIabES pAb L UNIaEbSITE

CONTbOLE CONT*OLE CONTROLE
b->R

Attaque statistique : que signifie NAoIONAhn

LA CrAbTE sU CONTbOLE sES CONNAISSANCES S AppLIiUE AUX sl pLOjES NATIONAUX sE LICENCE ET jASTEb ET AUX slpLOjES INT EbjEslAlbES sE sEUy ET jAITblSE sELIabES pAb L UNIaEbSITE

CONTbOLE CONT*OLE CONTROLE
b->R
UNIaERSITE UNIVERSITE

Attaque statistique : que signifie NAoIONAhn

LA CrAbTE sU CONTbOLE sES CONNAISSANCES S AppLIiUE AUX sl pLOjES NATIONAUX sE LICENCE ET jASTEb ET AUX slpLOjES INT EbjEslAlbES sE sEUy ET jAITblSE sELIabES pAb L UNIaEbSITE

CONTbOLE CONT*OLE CONTROLE
b->R
UNIaERSITE UNIVERSITE
a->V

Attaque statistique : que signifie NAoIONAhn

LA CrAbTE sU CONTbOLE sES CONNAISSANCES S AppLIiUE AUX sl pLOjES NATIONAUX sE LICENCE ET jASTEb ET AUX slpLOjES INT EbjEslAlbES sE sEUy ET jAITblSE sELIabES pAb L UNIaEbSITE

CONTbOLE CONT*OLE CONTROLE
b->R
UNIaERSITE UNIVERSITE
a->V
sELIVRES DELIVRES

Attaque statistique : que signifie NAoIONAhn

LA CrAbTE sU CONTbOLE sES CONNAISSANCES S AppLIiUE AUX sl pLOjES NATIONAUX sE LICENCE ET jASTEb ET AUX slpLOjES INT EbjEslAlbES sE sEUy ET jAITblSE sELIabES pAb L UNIaEbSITE

CONTbOLE CONT*OLE CONTROLE
b->R
UNIaERSITE UNIVERSITE
a->V
sELIVRES DELIVRES
s->D

Attaque statistique : que signifie NAoIONAhn

LA CrAbTE sU CONTbOLE sES CONNAISSANCES S AppLIiUE AUX sl pLOjES NATIONAUX sE LICENCE ET jASTEb ET AUX slpLOjES INT EbjEslAlbES sE sEUy ET jAITblSE sELIabES pAb L UNIaEbSITE

CONTbOLE CONT*OLE CONTROLE
b->R
UNIaERSITE UNIVERSITE
a->V
sELIVRES DELIVRES
s->D

LA CrARTE DU CONTROLE DES CONNAISSANCES S AppLIiUE AUX DI pLOjES NATIONAUX DE LICENCE ET jASTER ET AUX DIpLOjES INT ERjEDIAIRES DE DEUy ET jAITRISE DELIVRES pAR L UNIVERSITE

Chiffrement de Vernam

Gilbert Sandford Vernam (1880-1960) a inventé le *masque jetable*.

Première étape : transformer le message clair en suite de 0 et de 1. Plusieurs standards. Par exemple ASCII (American Standard Code for Information Interchange).

P est codé 1010000, Q est 1010001, R est 1010010, ...

Chiffrement de Vernam

Gilbert Sandford Vernam (1880-1960) a inventé le *masque jetable*.

Première étape : transformer le message clair en suite de 0 et de 1. Plusieurs standards. Par exemple ASCII (American Standard Code for Information Interchange).

P est codé 1010000, Q est 1010001, R est 1010010, ...

Question : Combien de caractères différents peut on coder avec ce standard ?

Chiffrement de Vernam

Gilbert Sandford Vernam (1880-1960) a inventé le *masque jetable*.

Première étape : transformer le message clair en suite de 0 et de 1. Plusieurs standards. Par exemple ASCII (American Standard Code for Information Interchange).

P est codé 1010000, Q est 1010001, R est 1010010, ...

Question : Combien de caractères différents peut on coder avec ce standard ?
Réponse : $2 \times 2 \times \ldots 2 = 2^7 = 128$.

Deuxième étape : On définit une opération $\oplus$ sur l'ensemble $\{0,1\}$ par

$\oplus$	0	1
0	0	1
1	1	0

Chiffrement de Vernam

Deuxième étape : On définit une opération $\oplus$ sur l'ensemble $\{0,1\}$ par

$\oplus$	0	1
0	0	1
1	1	0

$$m = 00101100100101010 01$$

Deuxième étape : On définit une opération $\oplus$ sur l'ensemble $\{0,1\}$ par

$\oplus$	0	1
0	0	1
1	1	0

$$\begin{aligned} m &= 00101100100101010 01 \\ k &= 10100110101001010 11 \end{aligned}$$

Deuxième étape : On définit une opération $\oplus$ sur l'ensemble $\{0,1\}$ par

$\oplus$	0	1
0	0	1
1	1	0

$$\begin{aligned} m &= 00101100100101010 01 \\ k &= 10100110101001010 11 \\ c = m \oplus k &= 10001010001100000 10 \end{aligned}$$

Chiffrement de Vernam

Deuxième étape : On définit une opération $\oplus$ sur l'ensemble $\{0,1\}$ par

$\oplus$	0	1
0	0	1
1	1	0

$$\begin{aligned} m &= 00101100100101010 01 \\ k &= 10100110101001010 11 \\ c = m \oplus k &= 10001010001100000 10 \end{aligned}$$

Question : comment retrouver m si on connaît k ?

Chiffrement de Vernam

Deuxième étape : On définit une opération $\oplus$ sur l'ensemble $\{0,1\}$ par

$\oplus$	0	1
0	0	1
1	1	0

$$\begin{aligned} m &= 00101100100101010 01 \\ k &= 10100110101001010 11 \\ c = m \oplus k &= 10001010001100000 10 \end{aligned}$$

Question : comment retrouver m si on connaît k ?

$$c = 10001010001100000 10$$

Chiffrement de Vernam

Deuxième étape : On définit une opération $\oplus$ sur l'ensemble $\{0,1\}$ par

$\oplus$	0	1
0	0	1
1	1	0

$$\begin{aligned} m &= 00101100100101010 01 \\ k &= 10100110101001010 11 \\ c = m \oplus k &= 10001010001100000 10 \end{aligned}$$

Question : comment retrouver m si on connaît k ?

$$\begin{aligned} c &= 10001010001100000 10 \\ k &= 10100110101001010 11 \end{aligned}$$

Chiffrement de Vernam

Deuxième étape : On définit une opération $\oplus$ sur l'ensemble $\{0,1\}$ par

$\oplus$	0	1
0	0	1
1	1	0

$$\begin{aligned} m &= 0010110010010101001 \\ k &= 1010011010100101011 \\ c = m \oplus k &= 1000101000110000010 \end{aligned}$$

Question : comment retrouver m si on connaît k ?

$$\begin{aligned} c &= 1000101000110000010 \\ k &= 1010011010100101011 \\ m = c \oplus k &= 0010110010010101001 \end{aligned}$$

Chiffrement de Vernam

Important : la clé est aussi longue que le message. Elle ne sert qu'une fois.

Question : montrez qu'un attaquant qui retrouve le message à partir du chiffré connaît forcément la clé.

Chiffrement de Vernam

Important : la clé est aussi longue que le message. Elle ne sert qu'une fois.

Question : montrez qu'un attaquant qui retrouve le message à partir du chiffré connaît forcément la clé.

$$k = c \oplus m.$$

Chiffrement de Vernam

Important : la clé est aussi longue que le message. Elle ne sert qu'une fois.

Question : montrez qu'un attaquant qui retrouve le message à partir du chiffré connaît forcément la clé.

$$k = c \oplus m.$$

Les informaticiens disent que ce chiffrement est *sémantiquement sûr*.

Chiffrement de Vernam

Important : la clé est aussi longue que le message. Elle ne sert qu'une fois.

Question : montrez qu'un attaquant qui retrouve le message à partir du chiffré connaît forcément la clé.

$$k = c \oplus m.$$

Les informaticiens disent que ce chiffrement est *sémantiquement sûr*.
Question : où est le problème ?

Chiffrement à clé publique

Alice 

Chiffrement à clé publique

Alice 
veut envoyer m à Bob.

Chiffrement à clé publique

Alice 

veut envoyer m à Bob.

Elle trouve la clé publique de chiffrement K^{pub}_{Bob} dans l'annuaire.

Chiffrement à clé publique

Alice 

veut envoyer m à Bob.

Elle trouve la clé publique de chiffrement K^{pub}_{Bob} dans l'annuaire.

Elle calcule $c = f_{K^{pub}_{Bob}}(m)$

Chiffrement à clé publique

Alice 

veut envoyer m à Bob.
Elle trouve la clé publique de chiffrement K_{Bob}^{pub} dans l'annuaire.
Elle calcule $c = f_{K_{Bob}^{pub}}(m)$

c est envoyé

Chiffrement à clé publique

Alice 

veut envoyer m à Bob.

Elle trouve la clé publique de chiffrement K^{pub}_{Bob} dans l'annuaire.

Elle calcule $c = f_{K^{pub}_{Bob}}(m)$

c est envoyé

à Bob 

Chiffrement à clé publique

Alice 

veut envoyer m à Bob.
Elle trouve la clé publique de chiffrement K_{Bob}^{pub} dans l'annuaire.
Elle calcule $c = f_{K_{Bob}^{pub}}(m)$

c est envoyé

à Bob 

c

Chiffrement à clé publique

Alice 

veut envoyer m à Bob.
Elle trouve la clé publique de chiffrement K_{Bob}^{pub} dans l'annuaire.
Elle calcule $c = f_{K_{Bob}^{pub}}(m)$

c est envoyé

à Bob 

c

qui utilise sa clé secrète de déchiffrement K_{Bob}^{sec}

Chiffrement à clé publique

Alice 

veut envoyer m à Bob.
Elle trouve la clé publique de chiffrement K_{Bob}^{pub} dans l'annuaire.
Elle calcule $c = f_{K_{Bob}^{pub}}(m)$

c est envoyé

à Bob 

c

qui utilise sa clé secrète de déchiffrement K_{Bob}^{sec}

$$m = f_{K_{Bob}^{pub}}{}^{(-1)}(c) = g_{K_{Bob}^{sec}}(c)$$

Chiffrement à clé publique

- Trois étapes : création et publication de clés, chiffrement, déchiffrement
- Avantages : gestion de clé simplifiée, solidité mathématique
- Fragilités : plus lent, plus compliqué à implémenter

En pratique on combine les deux chiffrements : clé publique pour échanger une clé de session (secrète) qui servira à chiffrer à la volée.

Identification par mot de passe

Alice 

Identification par mot de passe

Alice 

mot de passe d'Alice BELOTE

Identification par mot de passe

Alice 

mot de passe d'Alice BELOTE

BELOTE est envoyé

Identification par mot de passe

Alice 

mot de passe d'Alice BELOTE

BELOTE est envoyé

à Bob 

Identification par mot de passe

Alice

mot de passe d'Alice BELOTE

BELOTE est envoyé

à Bob

mot de passe de Bob

Identification par mot de passe

Alice

mot de passe d'Alice BELOTE

BELOTE est envoyé

à Bob

mot de passe de Bob REBELOTE

Identification par mot de passe

Alice

mot de passe d'Alice BELOTE

BELOTE est envoyé

à Bob

mot de passe de Bob REBELOTE

REBELOTE est envoyé

Identification par mot de passe

Alice 

mot de passe d'Alice BELOTE

BELOTE est envoyé

à Bob

mot de passe de Bob REBELOTE

REBELOTE est envoyé à Alice

Identifaction par mot de passe

- Alice et Bob doivent convenir d'un mot de passe secret partagé (question secrète)
- Avantage : simple
- Fragilités : risque de réutilisation e.g. par un tiers, gestion de mots de passe

Identification sans divulgation de connaissance

Alice 

Identification sans divulgation de connaissance

Alice 

connaît un secret S_{Alice}

Identification sans divulgation de connaissance

Alice 

connaît un secret S_{Alice}

Bob 

Identification sans divulgation de connaissance

Alice connaît un secret S_{Alice}

Bob interroge Alice et se convainc qu'elle connaît bien le secret.

Identification sans divulgation de connaissance

Alice 
connaît un secret S_{Alice}

Bob 
interroge Alice et se convainc qu'elle connaît bien le secret.

À la fin de l'échange, Bob n'a rien appris sur ce secret !

Comment faire ?

Situations asymétriques : l'un saît l'autre pas.
Celui qui connaît le secret a un avantage (il peut déchiffrer, il peut se prouver).
Mesurer cet avantage : théorie de la complexité.
S'appuyer sur des problèmes difficiles.

La thèse de Turing-Church

Alan Turing

Alonzo Church

Complexité algorithmique

Complexité algorithmique

- Ajouter deux entiers naturels de n chiffres : Cn opérations élémentaires où C est une constante,

Complexité algorithmique

- Ajouter deux entiers naturels de n chiffres : Cn opérations élémentaires où C est une constante,
- Multiplier deux entiers naturels de n chiffres : Cn^2 opérations élémentaires,

Complexité algorithmique

- Ajouter deux entiers naturels de n chiffres : Cn opérations élémentaires où C est une constante,
- Multiplier deux entiers naturels de n chiffres : Cn^2 opérations élémentaires,
- Effectuer une division euclidienne : Cn^2 opérations élémentaires,

Complexité algorithmique

- Ajouter deux entiers naturels de n chiffres : Cn opérations élémentaires où C est une constante,
- Multiplier deux entiers naturels de n chiffres : Cn^2 opérations élémentaires,
- Effectuer une division euclidienne : Cn^2 opérations élémentaires,
- Calculer le pgcd : Cn^2 opérations élémentaires,

Comptez les opérations élémentaires dans les calculs suivants

Complexité algorithmique

Comptez les opérations élémentaires dans les calculs suivants

- $123456543 + 324156261$

Complexité algorithmique

Comptez les opérations élémentaires dans les calculs suivants

- $123456543 + 324156261$
- 123×345

Complexité algorithmique

Comptez les opérations élémentaires dans les calculs suivants

- $123456543 + 324156261$
- 123×345

Calculez le pgcd de 402 et 174.

Tests de primalité

Les nombres premiers : 2, 3, 5, 7, 11, 13, 17, 1009, ...
Savoir si un entier P est premier.

Pierre de Fermat

Agrawal, Kayal et Saxena

$$T = n^{6+\epsilon(n)}$$

où n est le nombre de chiffres décimaux de P.

Tests de primalité

Trouvez tous les nombres premiers entre 1 et 100.

Tests de primalité

Trouvez tous les nombres premiers entre 1 et 100.
Trouvez tous les nombres premiers entre 1000 et 1025.