

CS547A  
Cryptography and Data Security

Lecture 01

**Claude Crépeau**

School of Computer Science  
McGill University



Classical

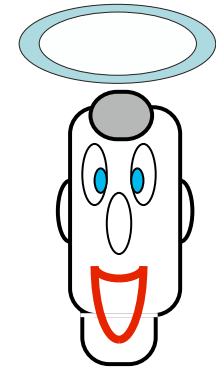
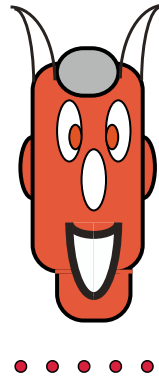
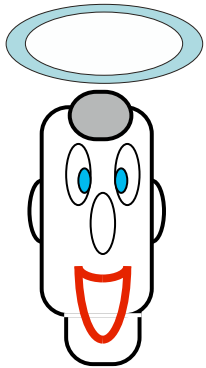
Cryptography

Information

Theoretical

Cryptography

# Information Theoretical Cryptography



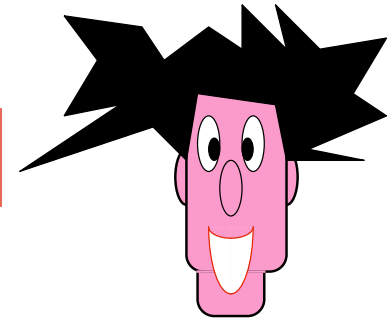
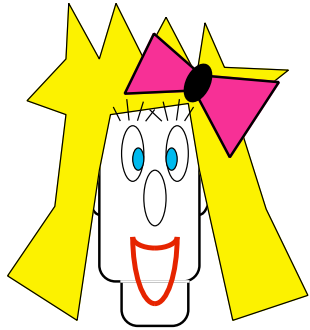
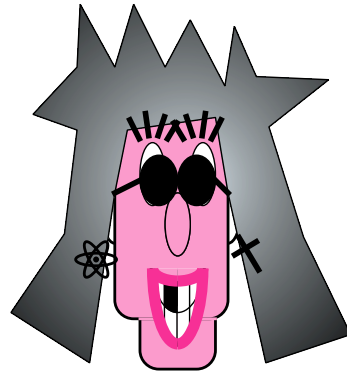
key distribution

encryption

authentication

identification





Will you marry me ?

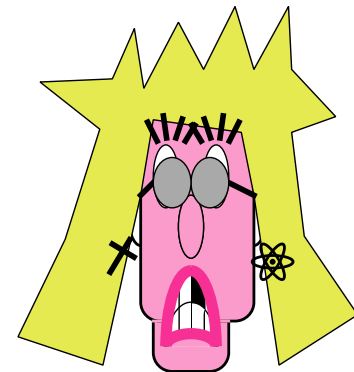
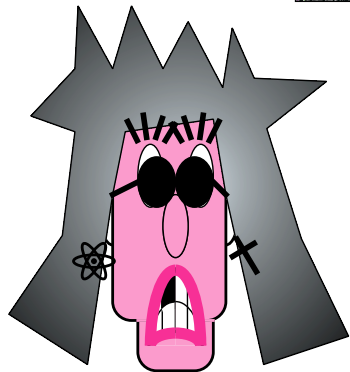
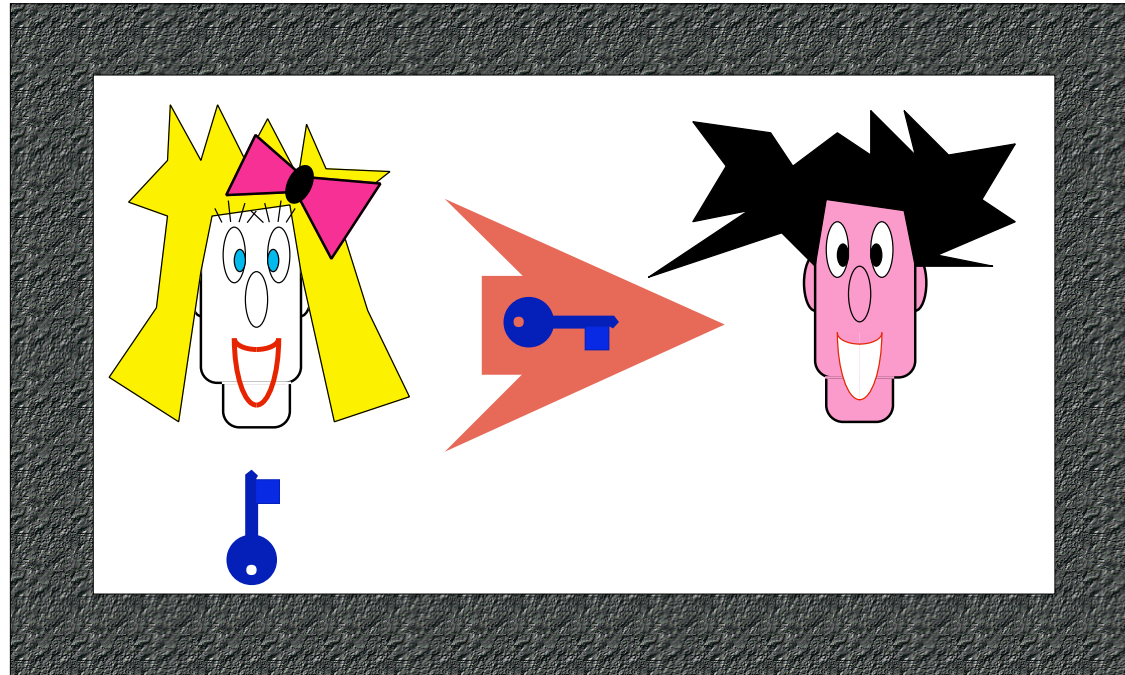
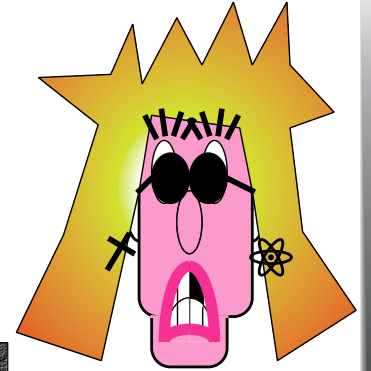
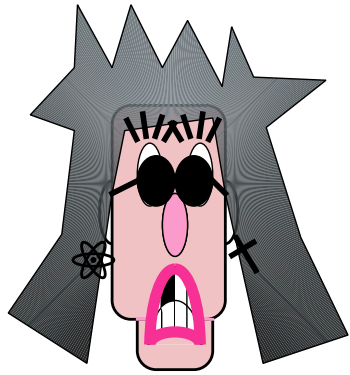
Divorce your wife first !

The papers are in the mail...

OK, I will !

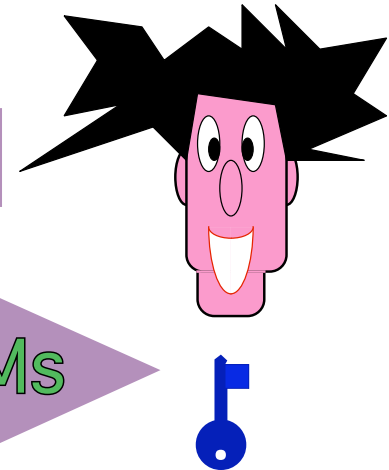
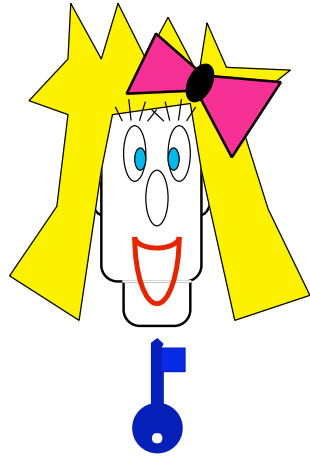
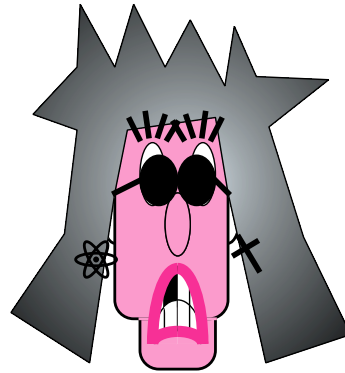
key

distribution



encryption





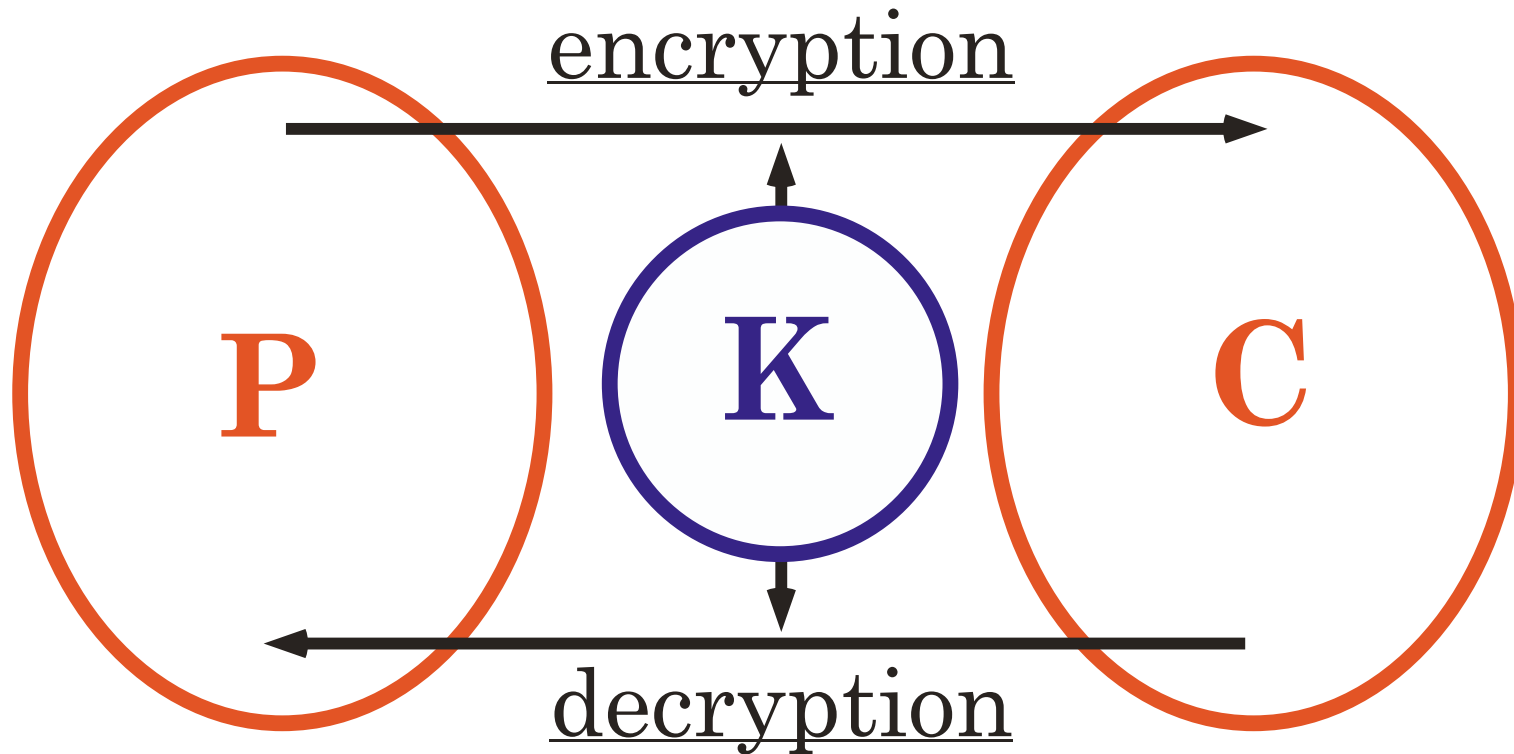
8RdewtU5qkLa\$es!T9@

I(D%eXhDqliykl#2cV7dEwnMs

H&fs@tyHvFGhaOKpTrGbl.Z/rUih\*

B7B3tdsjUila

# symmetric encryption

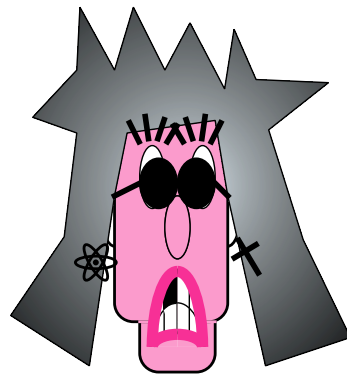
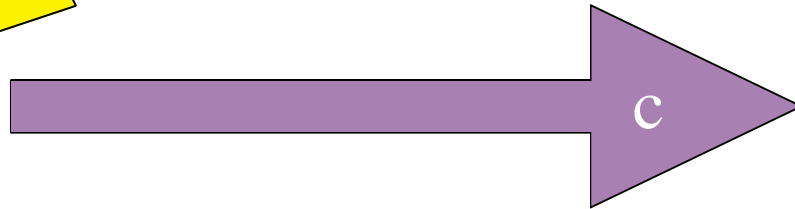
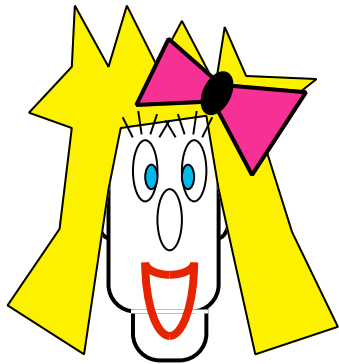


Information Theoretical Security

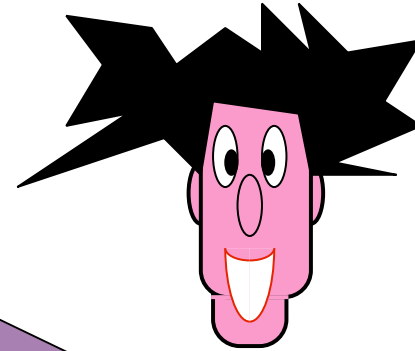


# Vernam's One-Time-Pad

m	k = c	
1	1	0
0	1	1
1	1	0
0	0	0
0	0	0
1	1	0
0	1	1
0	0	0
1	1	0
1	1	0
1	0	1
1	1	0
1	0	1
0	1	1
0	1	1
1	1	0

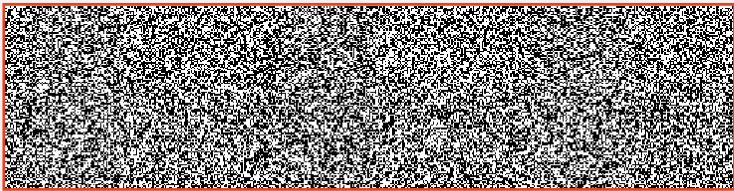


c	k = m	
0	1	1
1	1	0
0	1	1
0	0	0
0	0	0
0	1	1
1	1	0
0	0	0
0	1	1
0	1	1
1	0	1
0	1	1
1	0	1
1	1	0
1	1	0
0	1	1

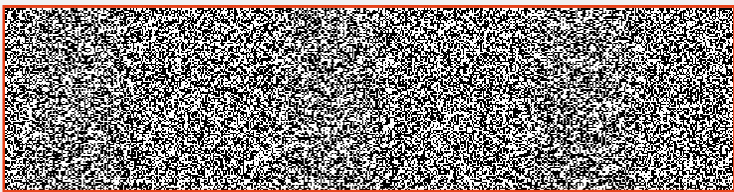


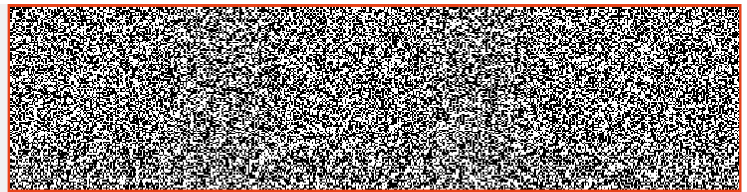
M **VERNAM**

⊕

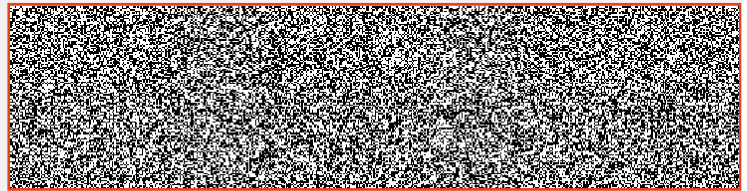
K 

=

C 

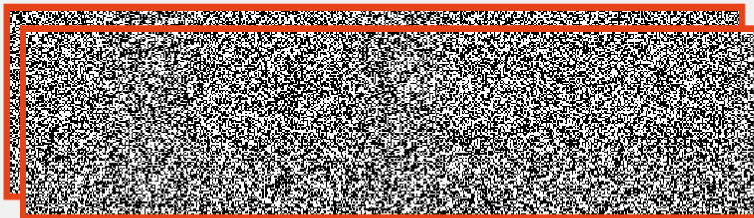
C 

⊕

K 

=

M **VERNAM**

C  K

=

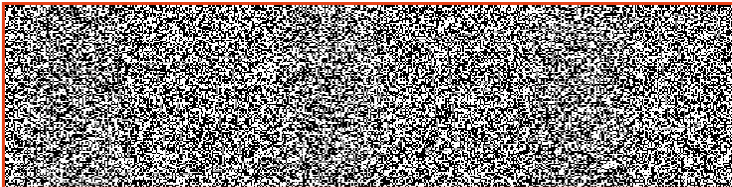
M' 

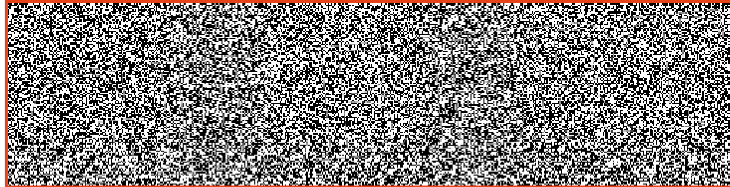
M GILBERT

$\oplus$

K 

=

C 

C 

$\oplus$

K 

=

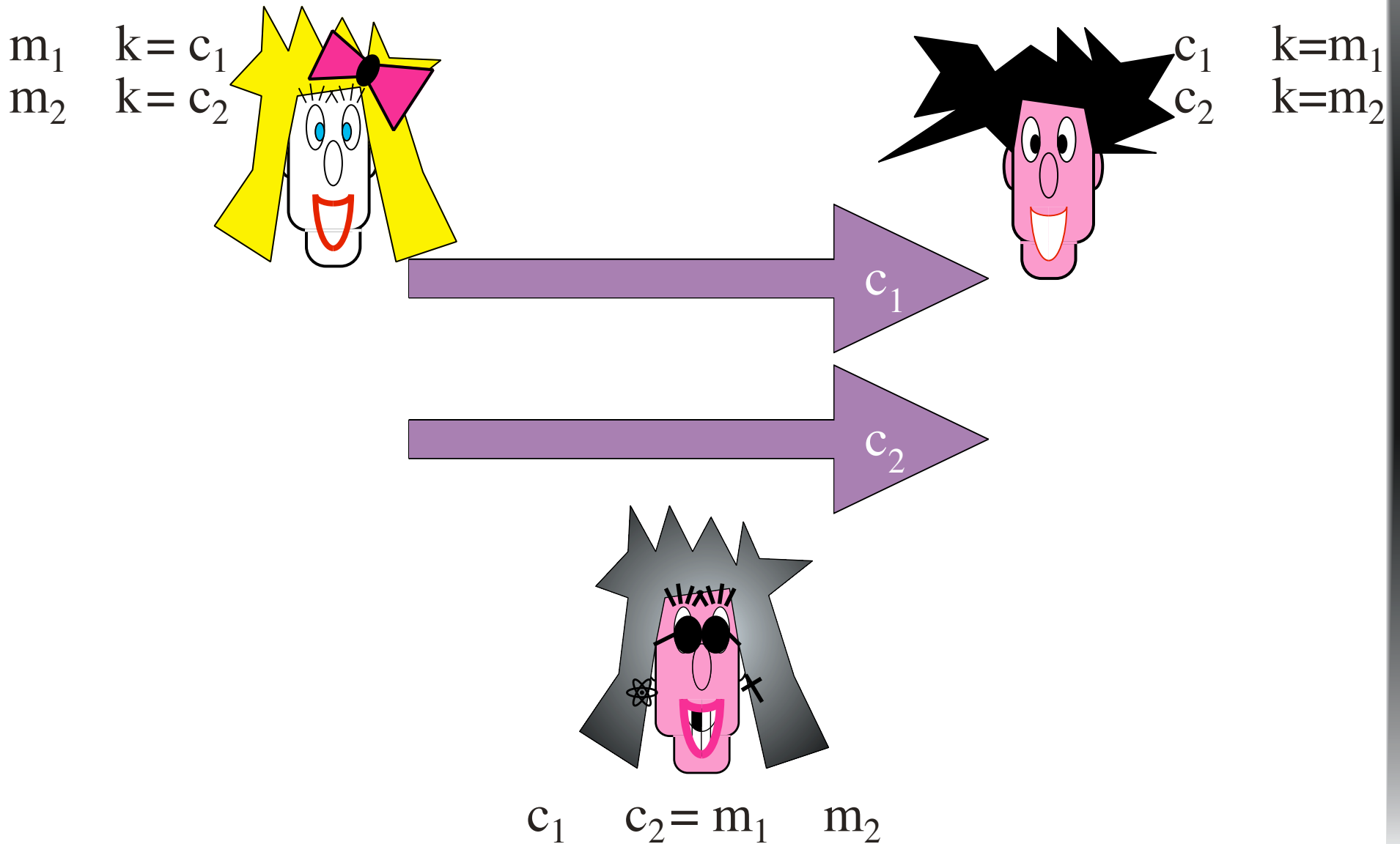
M GILBERT

C  K

=

M' 

# Vernam's One-Time-Pad



$M_0$  VERNAM

$\oplus$

$M_1$  GILBERT

=

$X$  GILBERT

$C_0$  [Noise]

$\oplus$

$C_1$  [Noise]

=

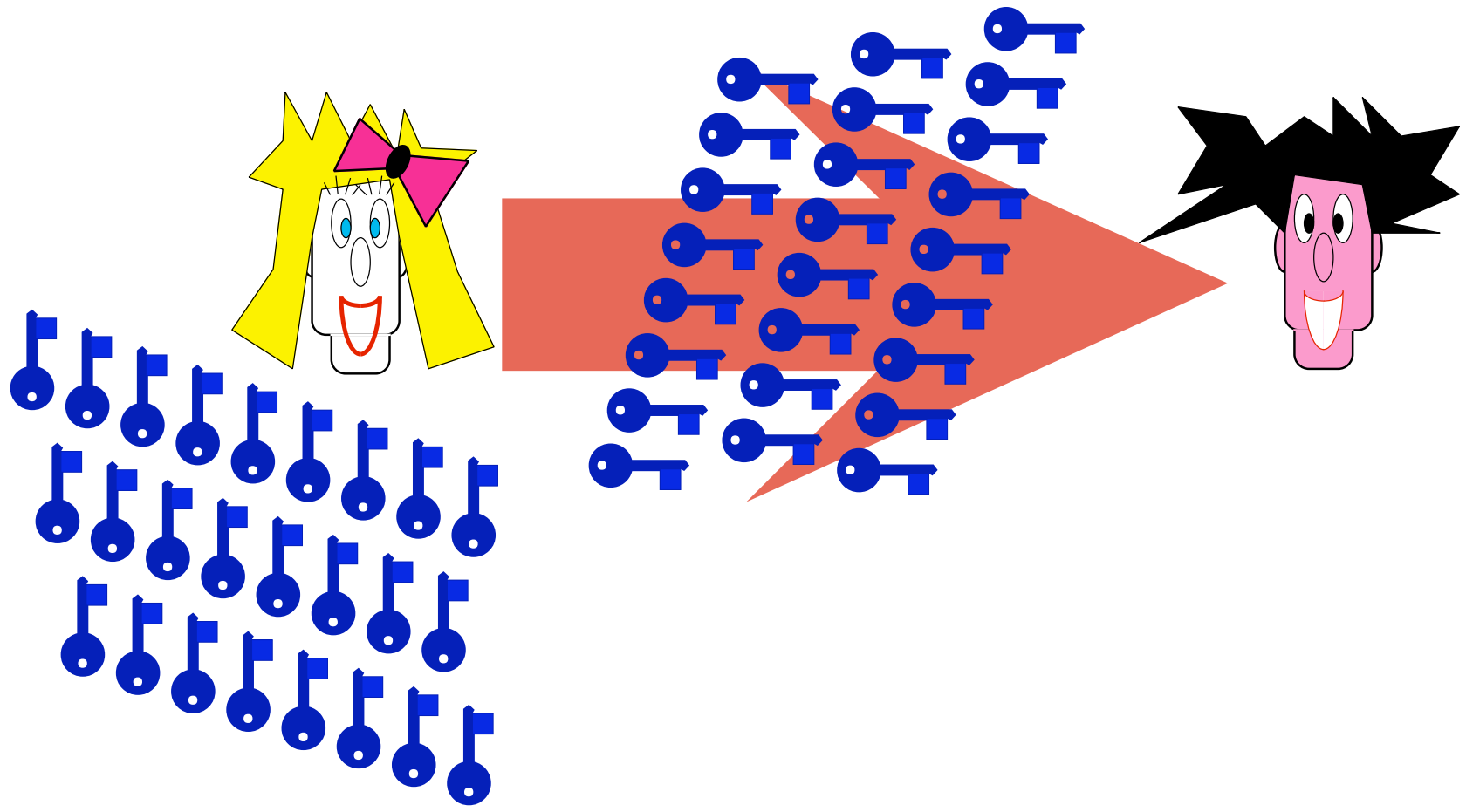
$X$  GILBERT

$C_0$  [Noise]  $C_1$

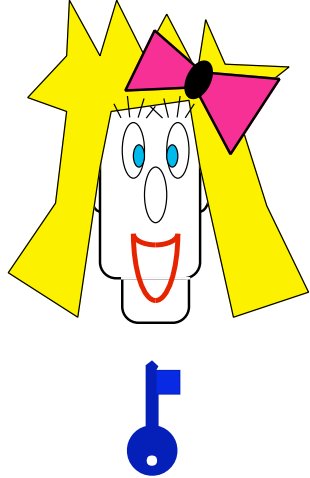
=

$X'$  GILBERT





authentication

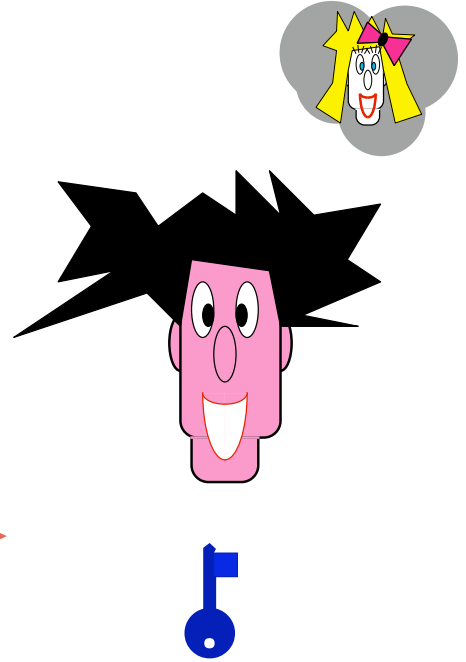


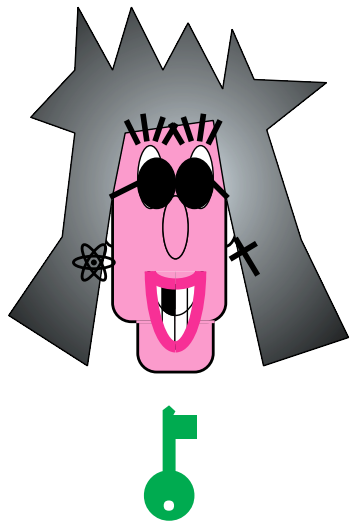
Will you marry me ?

Divorce your wife first !

The papers are in the mail...

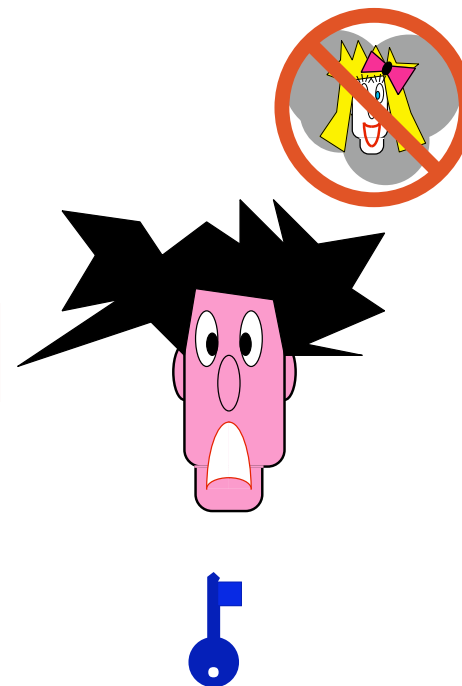
OK, I will !



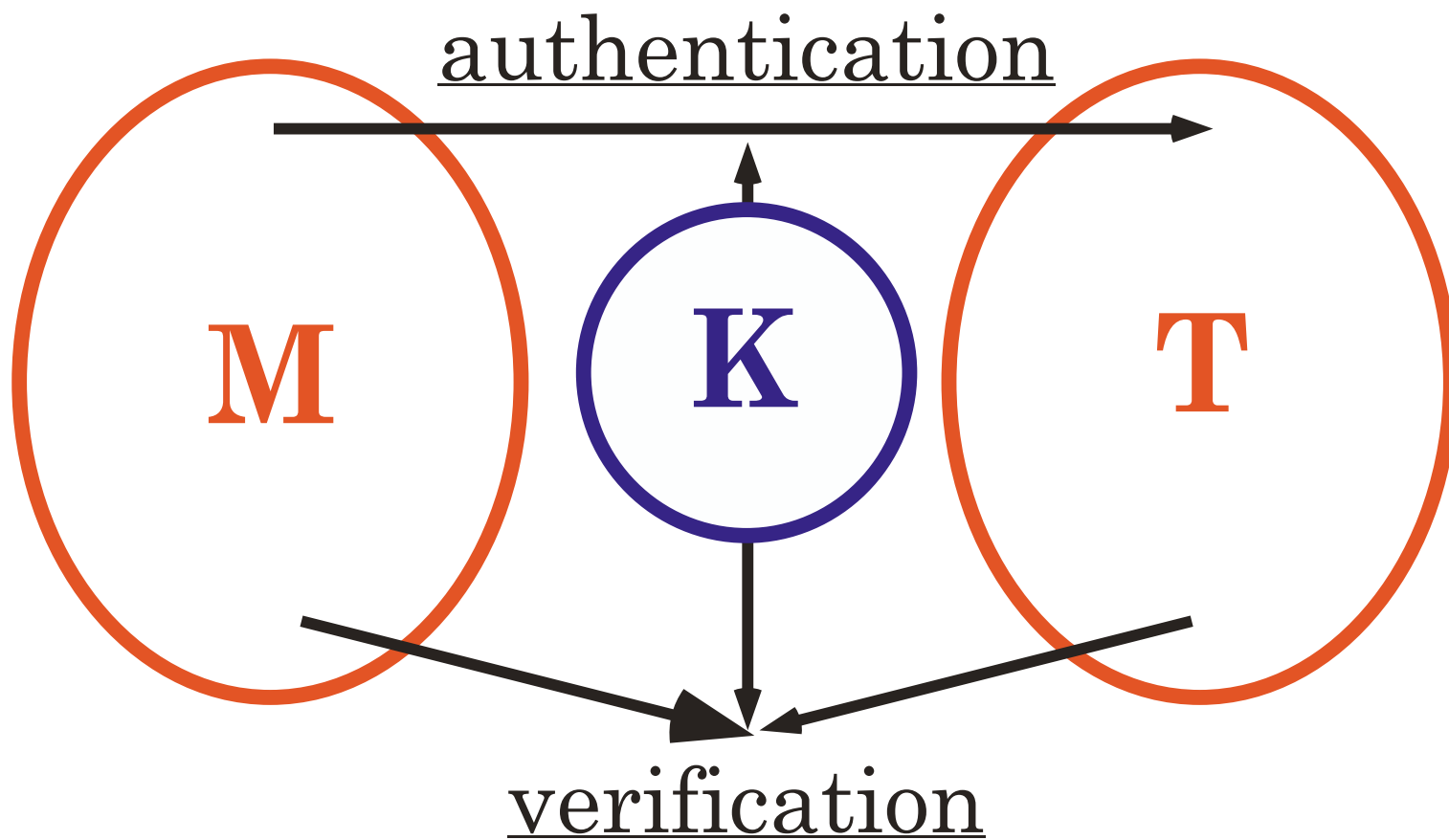


Will you marry me ?

No, I never will !

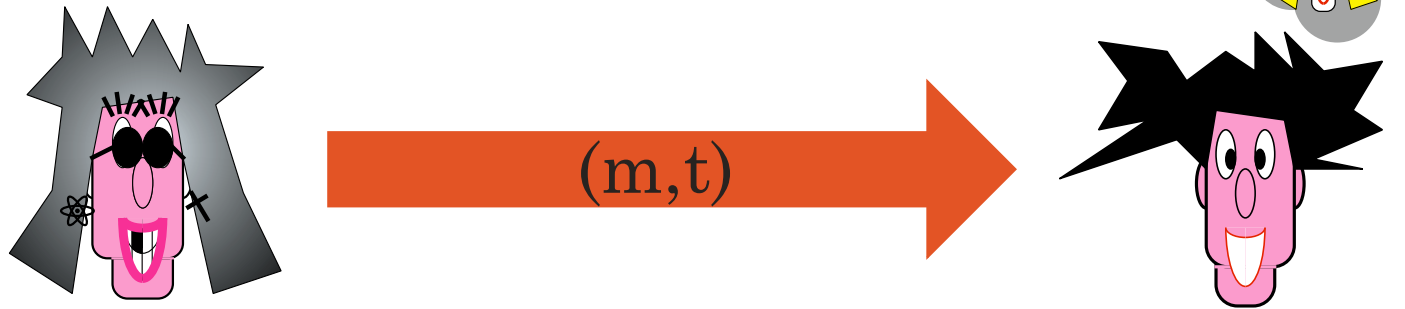


# symmetric authentication

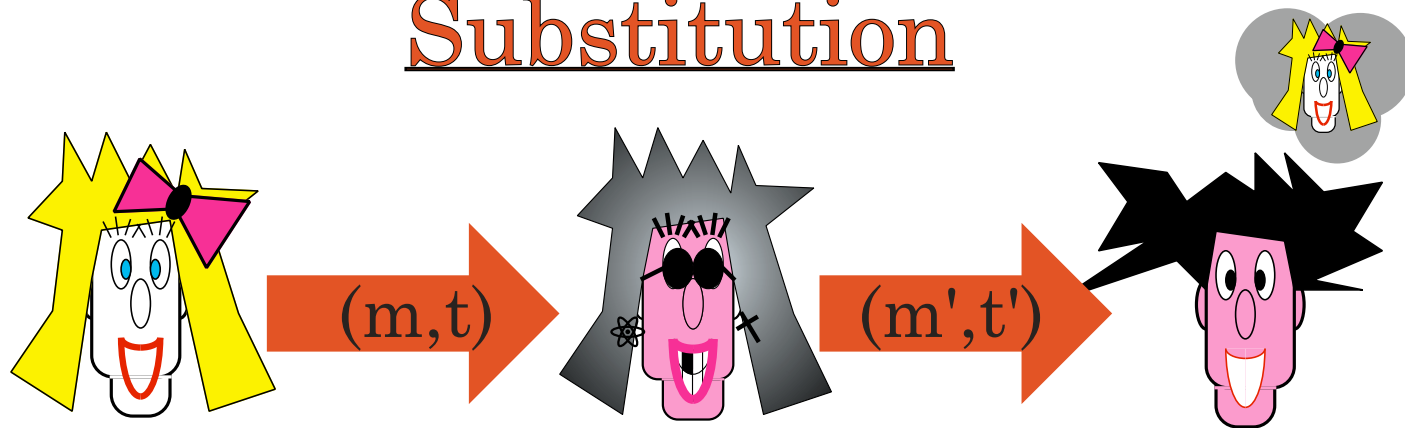


Information Theoretical Security

# Impersonation

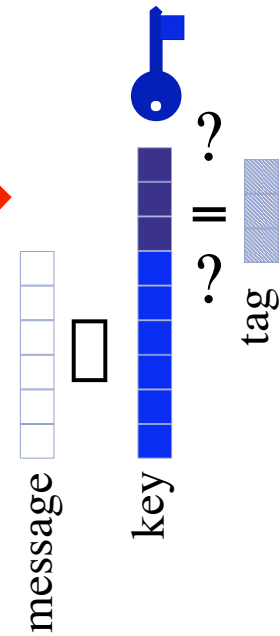
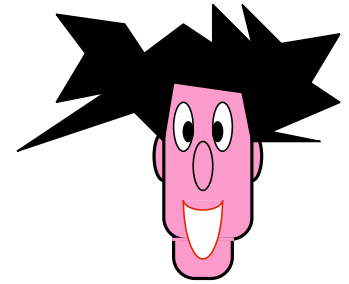
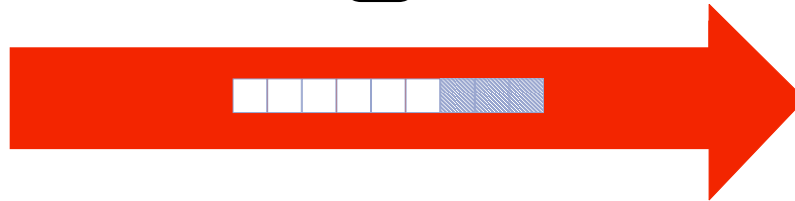
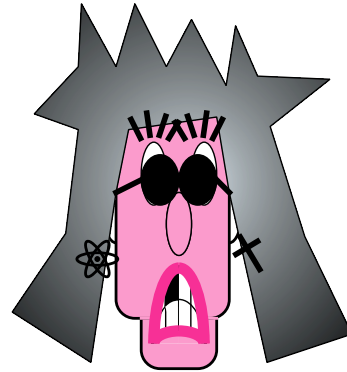
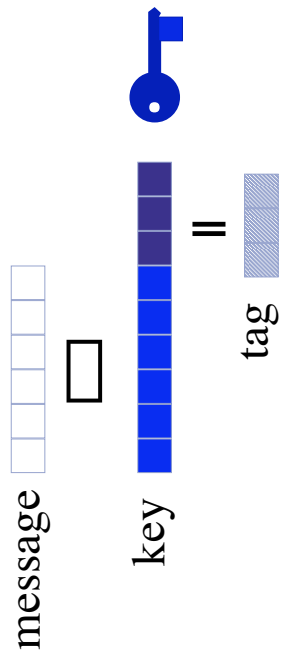
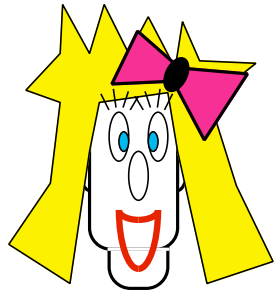


# Substitution



Information Theoretical Security

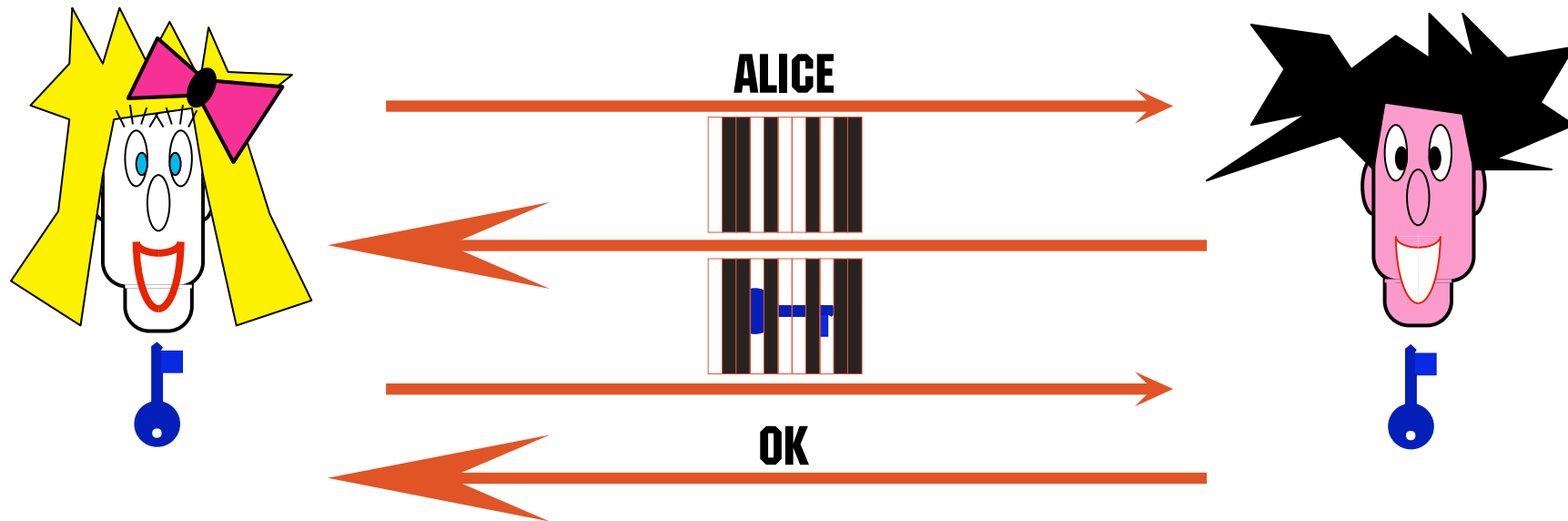
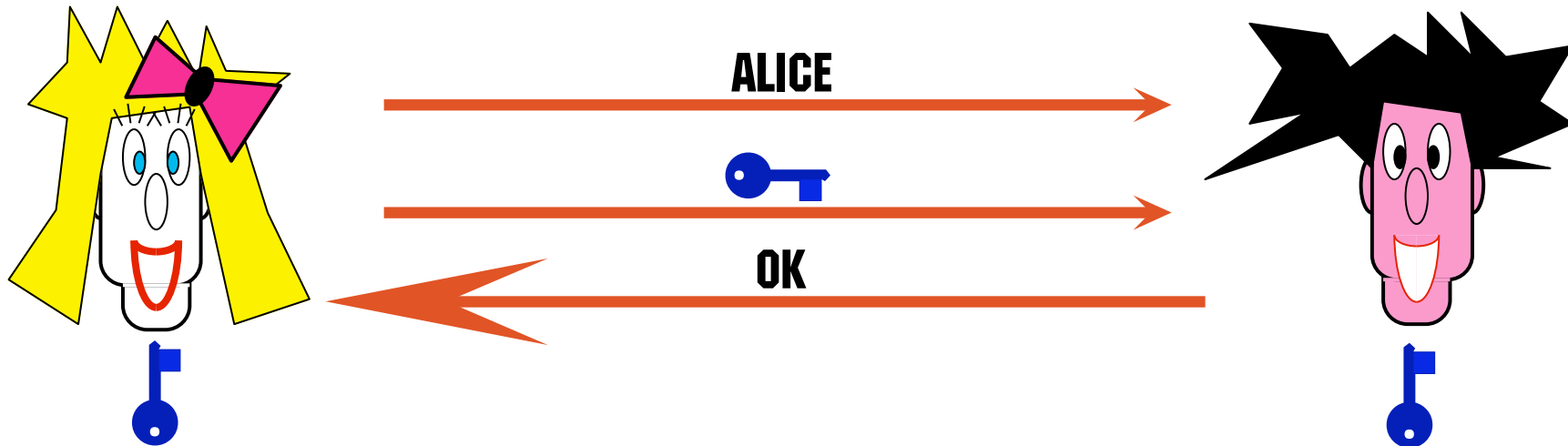
# One-Time-Authentication



identification



# one-time Identification





MONT-SAINT-HILAIRE

# Des fraudeurs déjouent la sécurité des cartes de débit

## (Crooks Bypass the Security of Debit Cards)

BERNARD LAN HART

Les policiers de Mont-Saint-Hilaire enquêtent sur une affaire de fraude comme il n'y en aurait jamais eu au Québec et qui pourrait compromettre sérieusement l'utilisation des cartes de débit bancaires.

Les fraudes, une dizaine au total, ont été commises jeudi de la semaine dernière, entre 18 h et 21 h, à l'intérieur du dépanneur Couche-Tard, du 670, boulevard Laurier, à Mont-Saint-Hilaire.

Les victimes sont des clients de ce commerce qui ont payé leur achat avec leur carte de débit automatique, sans savoir que le lecteur (skimmer) utilisé avait été trafiqué par les fraudeurs et installé dans le commerce avec la complicité du commis.

Pour payer leur achat, les clients ont présenté leur carte de débit et composé leur NIP, avant que le commis ne leur remette, comme si tout était normal, le petit reçu indiquant le montant de la transaction et indiquant que celle-ci avait été approuvée par l'institution bancaire.

Ce que les clients ne savaient pas, et qu'ils ne savent probablement toujours pas, c'est que le lecteur n'était pas branché au système Interac. Ils ne pouvaient pas imaginer non plus que l'appareil avait été trafiqué de façon à permettre aux fraudeurs d'enregistrer leur numéro de compte et leur numéro d'identification personnel (NIP).

### LE CRIME PRESQUE PARFAIT!

Comme le lecteur n'était branché à aucun système, le compte de banque des clients n'a jamais été débité pour l'achat effectué ce soir-là. Et pour être certain de ne laisser absolument aucune trace, le commis du dépanneur, selon les directives qui lui avaient été faites, enregistrait l'achat sur sa caisse comme s'il avait été payé comptant. Il

pas de plaignant et il n'y a absolument aucune trace de la fraude. Ça du jamais vu au Québec. Il s'agit d'une affaire qui a été mentionnée dans le journal. Le sergent-détective Bertrand Déry, de la Sécurité publique de Mont-Saint-Hilaire.

### UN AUTRE CAS

M. Déry recommande le plus grand des prudences avec les cartes de débit. Et il va même jusqu'à recommander l'utilisation. «Nous n'avons aucune idée de l'ampleur de

des cartes ont été... de commerces? Nous avons seulement qu'un commis d'un autre dépanneur Couche-Tard, celui du 315, Laurier à Mont-Saint-Hilaire, avait été approché par le même fraudeur une semaine plus tôt. Mais il avait refusé de se faire complice», précise M. Déry.

### JEUNE NOIR RECHERCHÉ

Les informations détenues par les policiers, qui s'apprentent à déposer des accusations de fraudes contre le commis du dépanneur, indiquent qu'un homme d'une vingtaine d'années, de race noire, faisant environ 5 pieds, huit pouces et 165 livres, se serait présenté au dépanneur du boulevard Laurier vers 18 h, le 8 mars, pour conclure un marché avec l'employé du commerce.

Il aurait offert 10 000 \$ à ce dernier pour brancher durant la soirée son «skimmer» trafiqué. L'employé aurait accepté et reçu sur-le-champ quelques centaines de dollars pour régler comptant les transactions.

Selon le commis, qui a été interrogé par le sergent-détective Déry, une dizaine de transactions seulement ont été effectuées avec le lecteur trafiqué. Et jusqu'à preuve du contraire, les comptes bancaires des clients, qui ne sont toujours pas identifiés, n'ont pas été vidés par les fraudeurs.

Arrêté par les policiers, le commis a expliqué qu'il n'a jamais touché les 10 000 \$ promis. Les fraudeurs ne lui auraient remis que 400 \$ pour ce service.

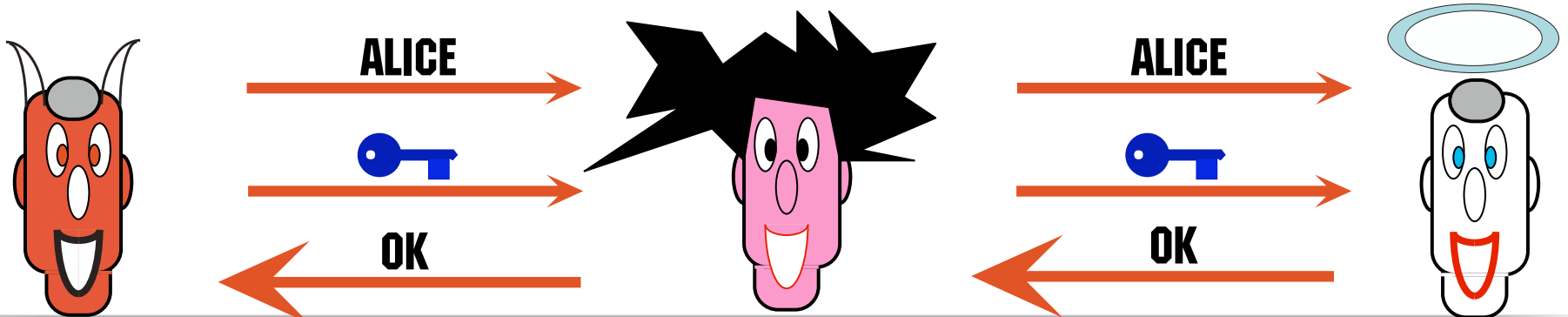
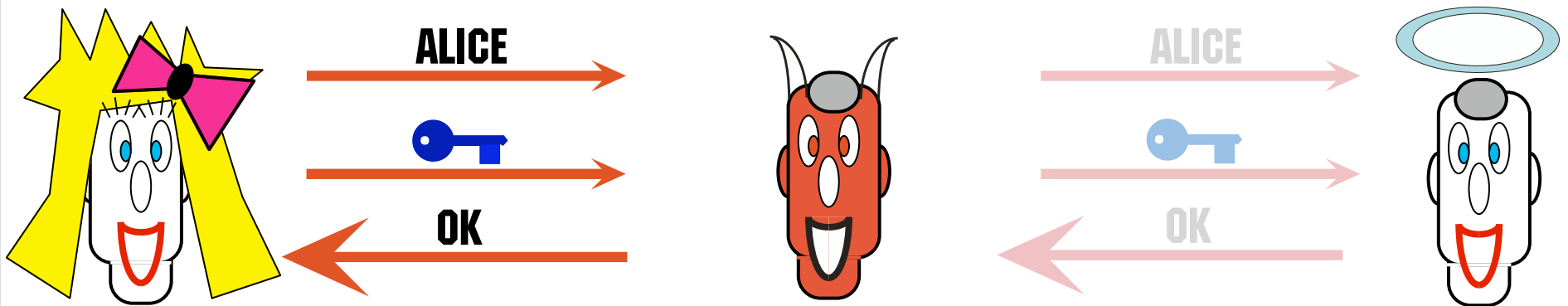
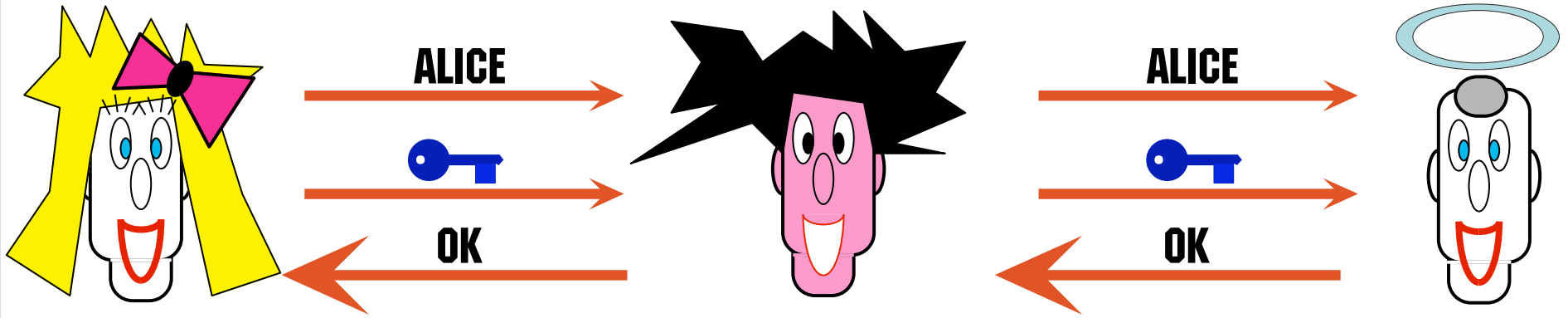
Tous les clients qui ont fréquenté le dépanneur Couche-Tard entre 18 h et 21 h le 8 mars sont invités à communiquer avec M. Déry au 467-3371.

Les policiers sont par ailleurs à la recherche du jeune homme de race noire d'une vingtaine d'années qui se déplace en compagnie de deux complices d'origine liba-



L'individu de race noire qui est recherché par les policiers avait fait une offre à un autre commis d'un dépanneur de Mont-Saint-Hilaire, une semaine avant de commettre ses fraudes.

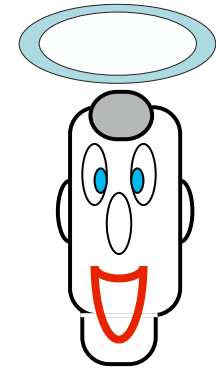
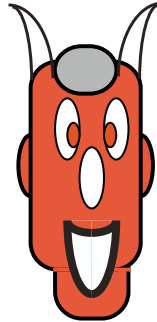
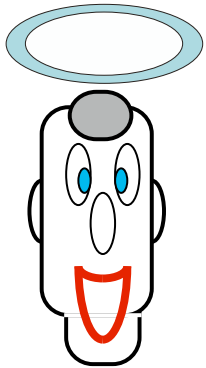
# Impersonation



Quantum

Cryptography

# Information Theoretical Cryptography



.....

## Quantum key distribution

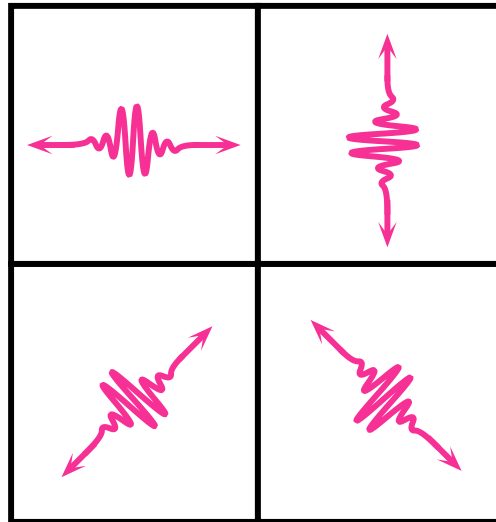
.....

# Ambiguous Coding Scheme

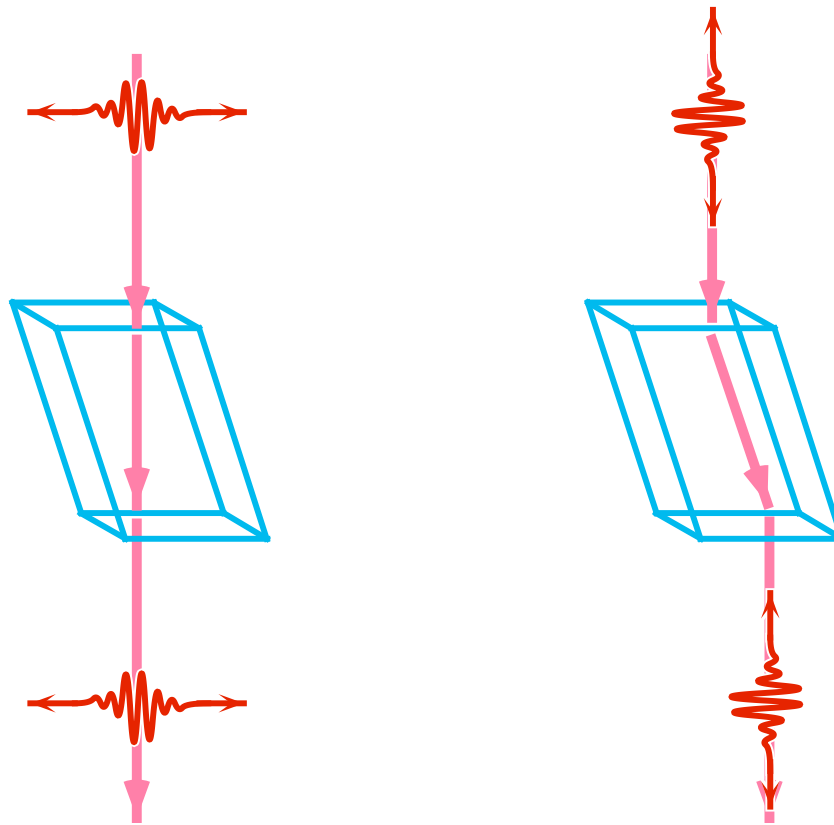
0 1

+

□

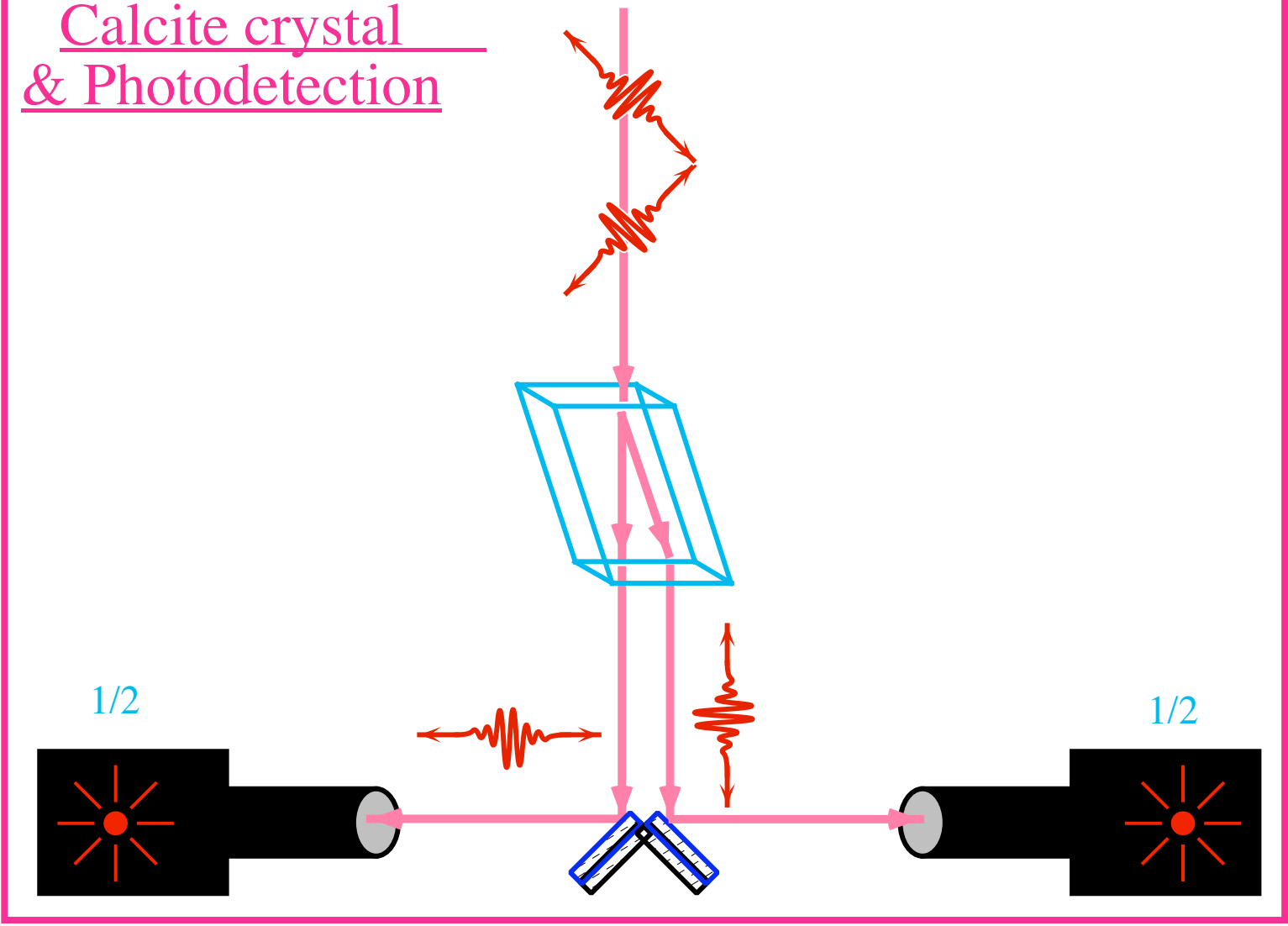


## Calcite crystal



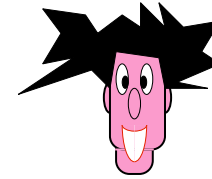
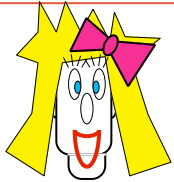


Calcite crystal  
& Photodetection



quantum key  
distribution

# Quantum-Key Distribution



☐:	0	1	1	0	0	1	0	0	1	1	0	1	0	0	0	1	1	1	0	1	1	0	0	0	
	☐	+	☐	+	+	+	☐	☐	☐	☐	+	+	+	+	☐	☐	☐	+	☐	+	+	+	☐	+	
☐:	☐	☐	+	+	☐	+	+	+	☐	+	+	☐	☐	☐	+	☐	☐	☐	+	+	☐	+	☐	+	
	0	0	1	0	0	1	0	0	1	0	0	0	0	0	1	1	1	0	0	0	1	1	0	0	0
☐:	☐	+	☐	+	+	+	☐	☐	☐	☐	+	+	+	+	☐	☐	☐	+	☐	+	+	+	☐	+	
☐:	0	☹	☹	0	☹	1	☹	☹	1	☹	0	☹	☹	☹	☹	1	0	☹	☹	1	☹	0	0	0	
☐:	0		0	1		1	0					1	0		1	0	0	0	0						
☐:	0		0	1		1	0					1	1		1	1	0	0	0						
☐:	0		1		0		1					1	1		1	1	0	0	0						
☐:	=		=		=																				
☐:		0		1		1						1	1		1	1	0	0							
☐:		0		1		1						1	1		1	1	0	0							

20%

## Bennett-Brassard

# Quantum-Key Distribution

.....

- Produces raw classical key
- Observed error rate indicates amount of eavesdropper information
- Error-correction is used to fix errors
- Random hash function is used to distill a smaller secret classical key

.....

CS547A  
Cryptography and Data Security

Lecture 01

**Claude Crépeau**

School of Computer Science  
McGill University



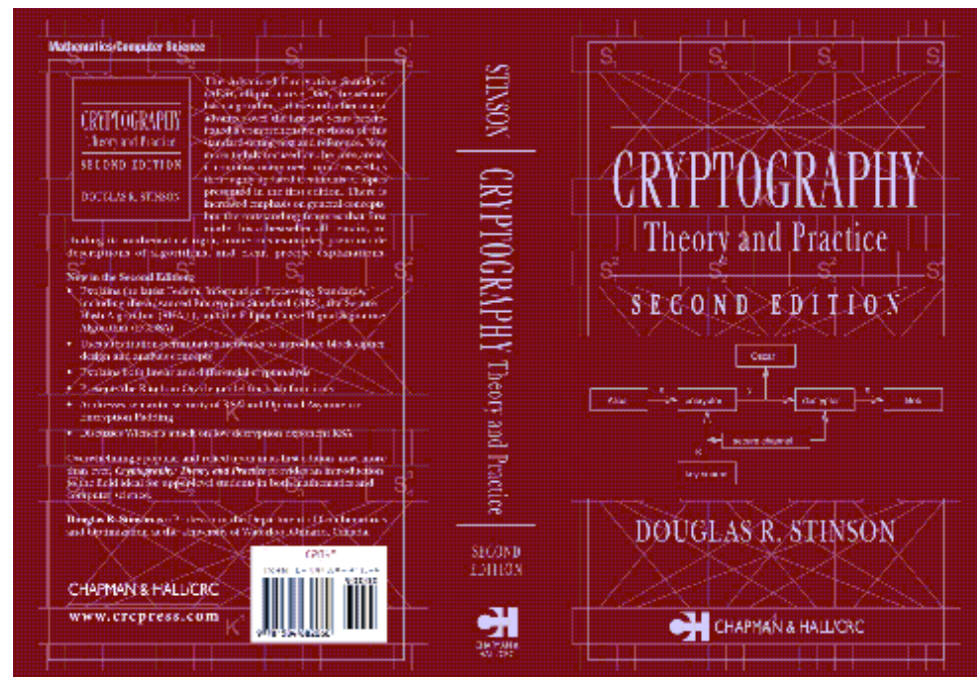
# Mandatory Material



- Class notes (course web page)

- Maple™ software

- Stinson's book



# Evaluation

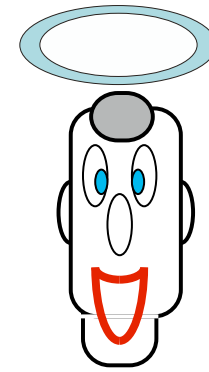
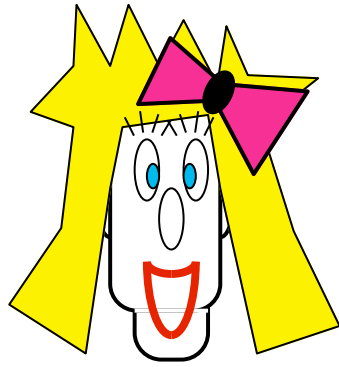


- Theoretical exercises : 30%

- Maple™ exercises : 20%

- FINAL EXAM : 50%





**CIAO !**

