COMP 102A, Lecture 15

Introduction to Cryptography

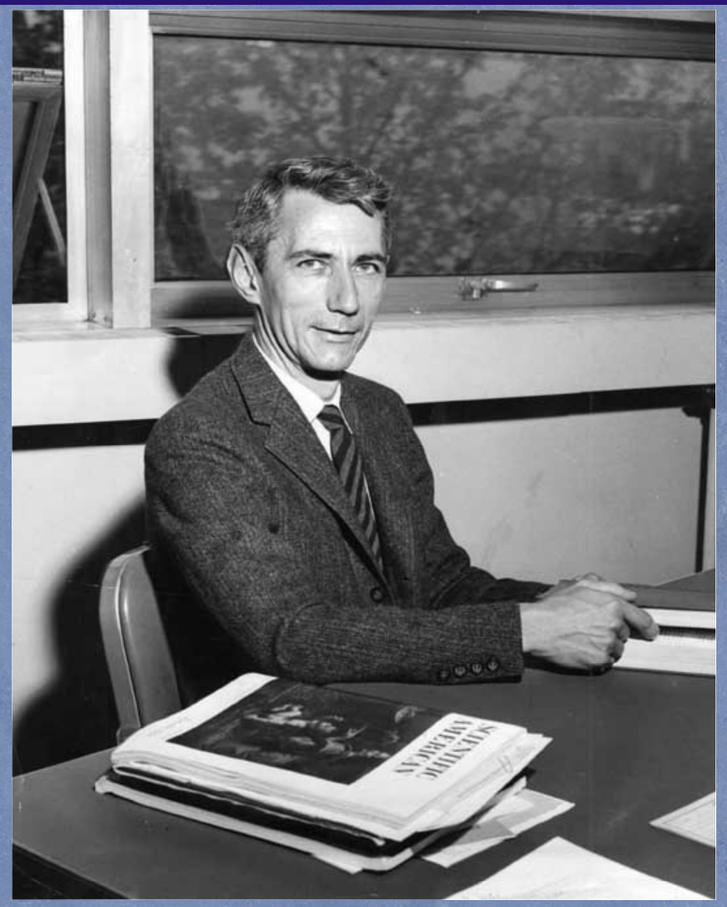
COMP 102A, Lecture 15

Classical

Cryptography

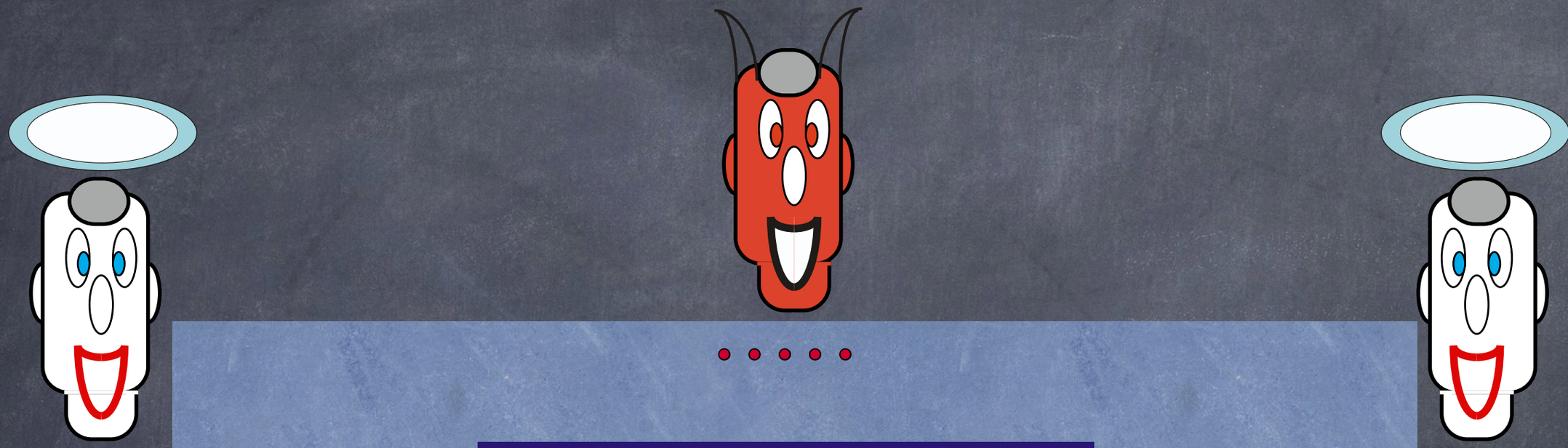
Information

Theoretical



Cryptography

Information Theoretical Cryptography



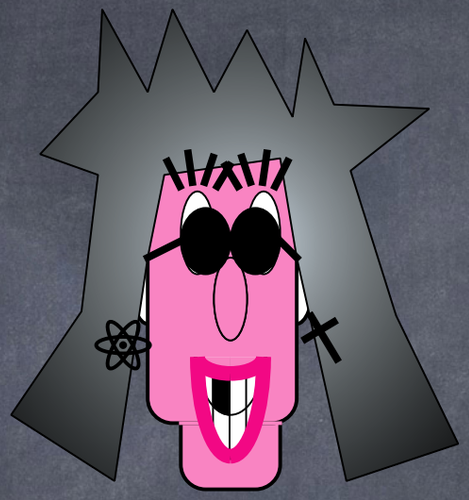
Key Distribution

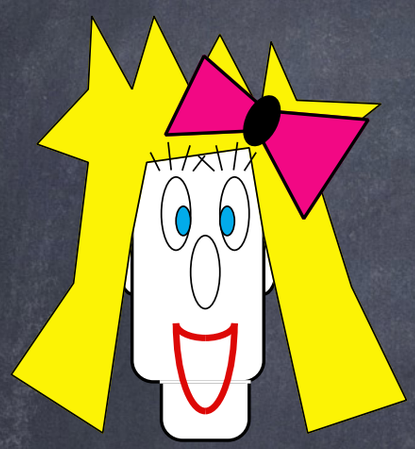
Encryption

Authentication

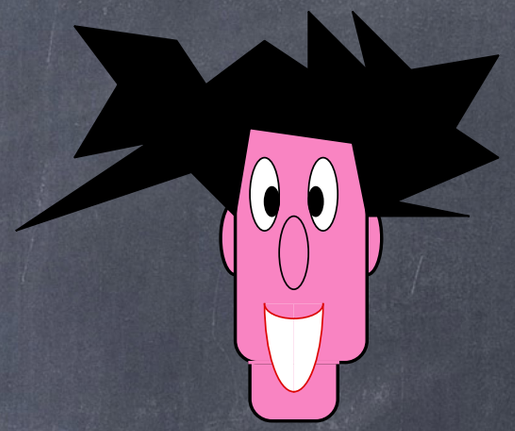
Identification

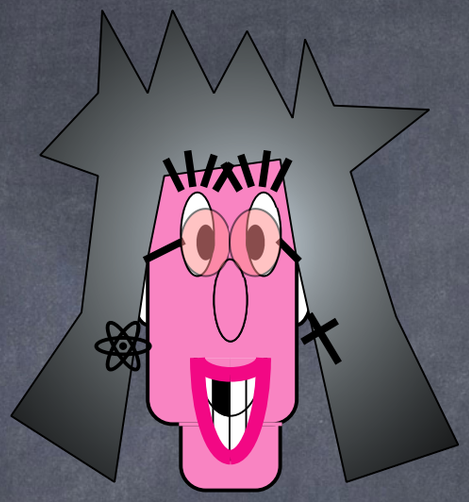
.....

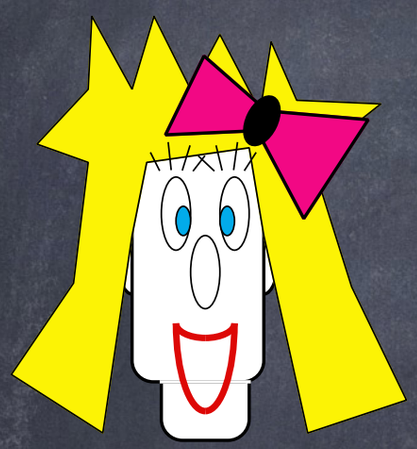




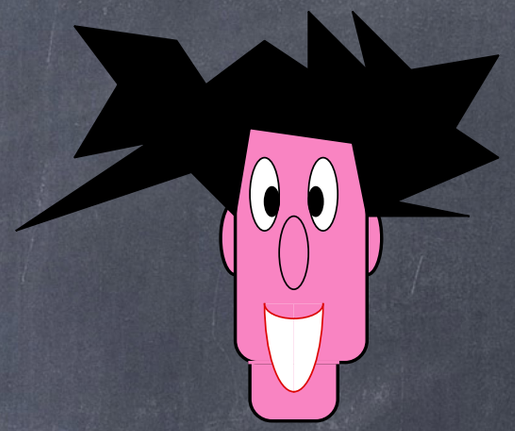
Will you marry me ?



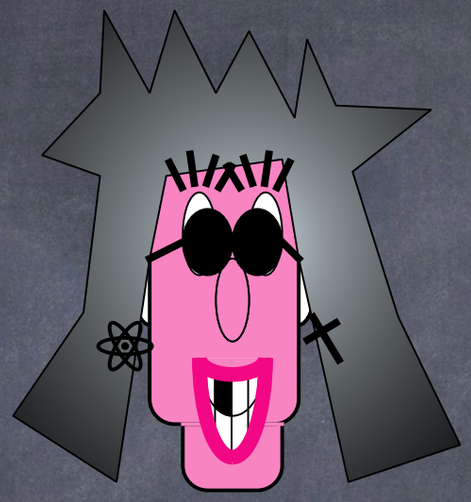


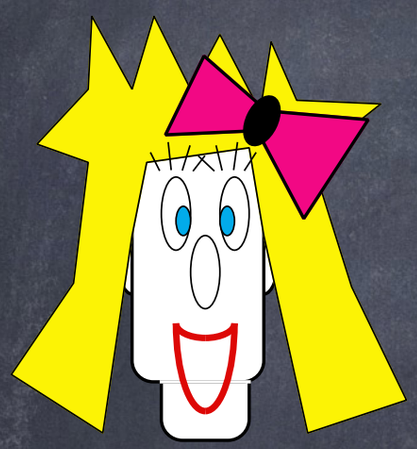


Will you marry me ?

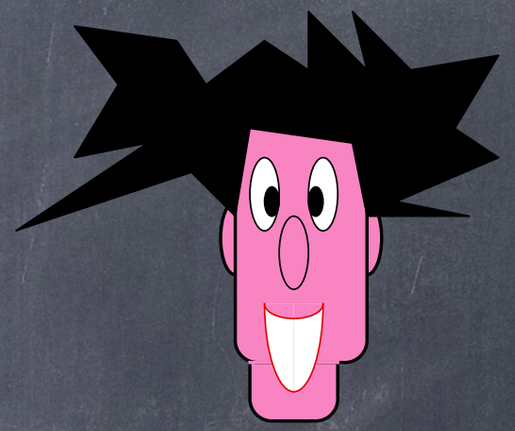


Divorce your wife first !



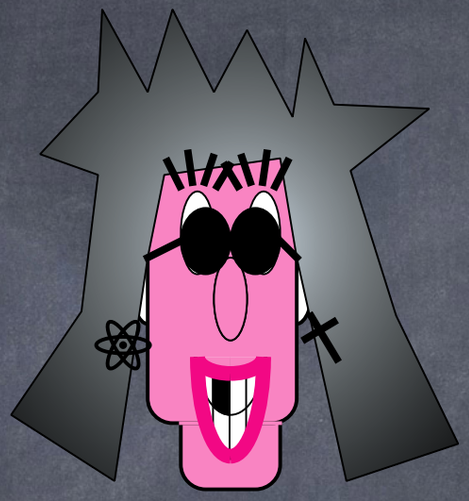


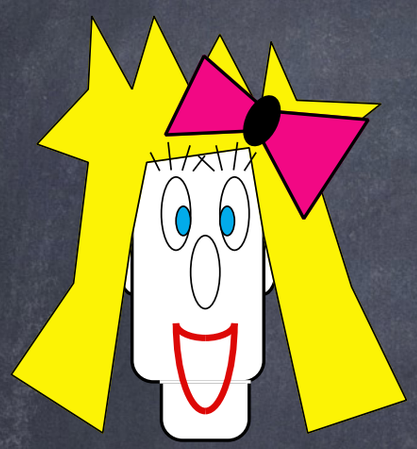
Will you marry me ?



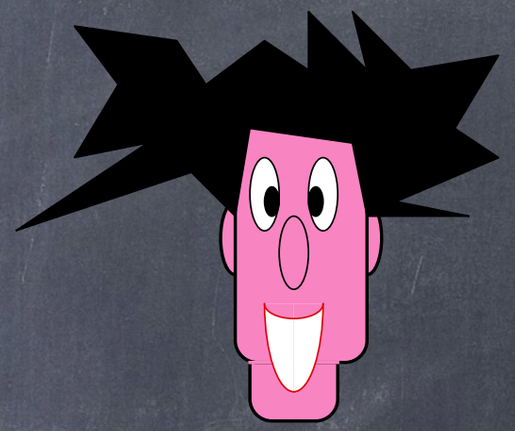
Divorce your wife first !

The papers are in the mail...





Will you marry me ?

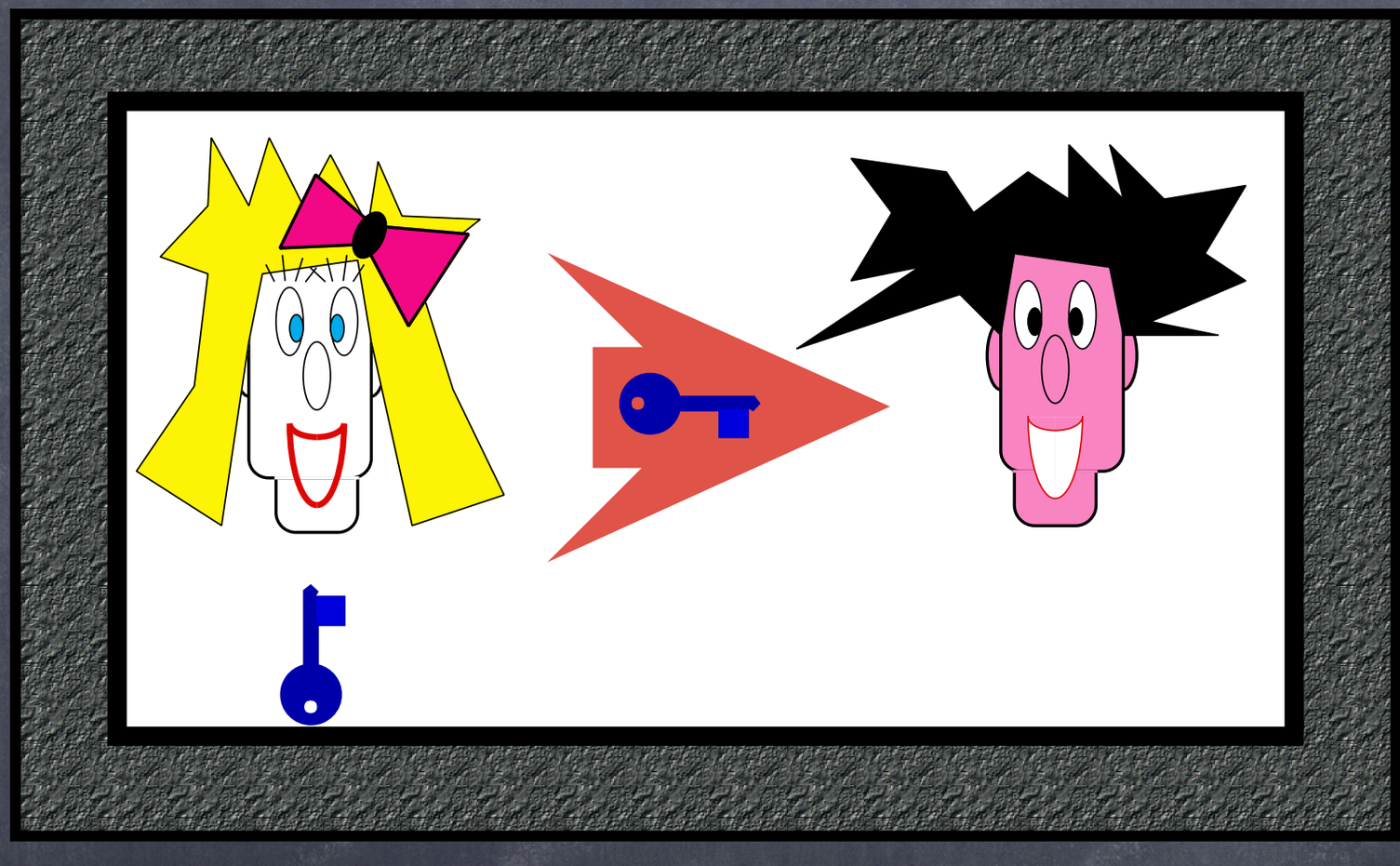


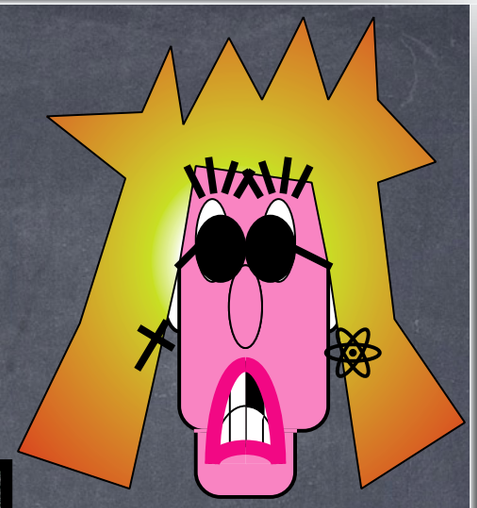
Divorce your wife first !

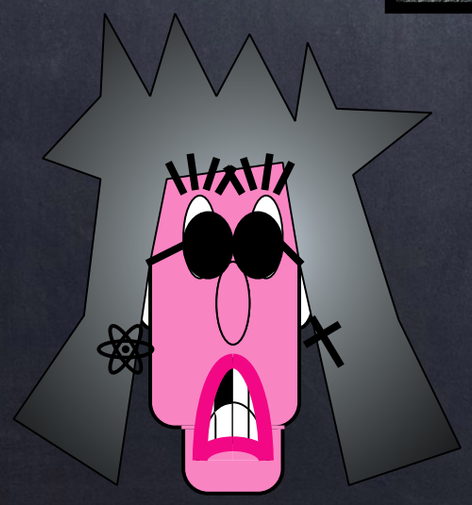
The papers are in the mail...

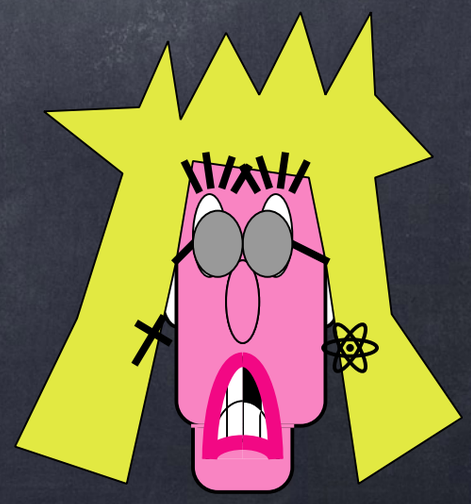
OK, I will !

Key Distribution

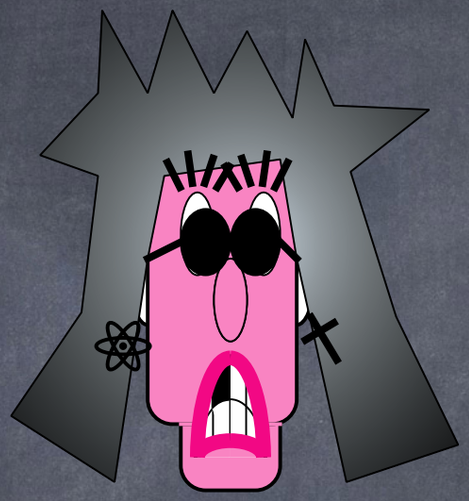


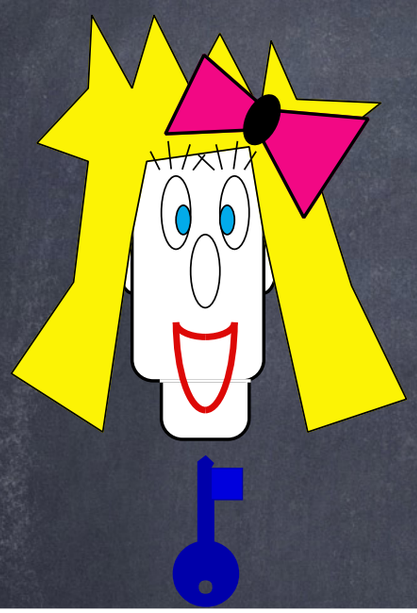




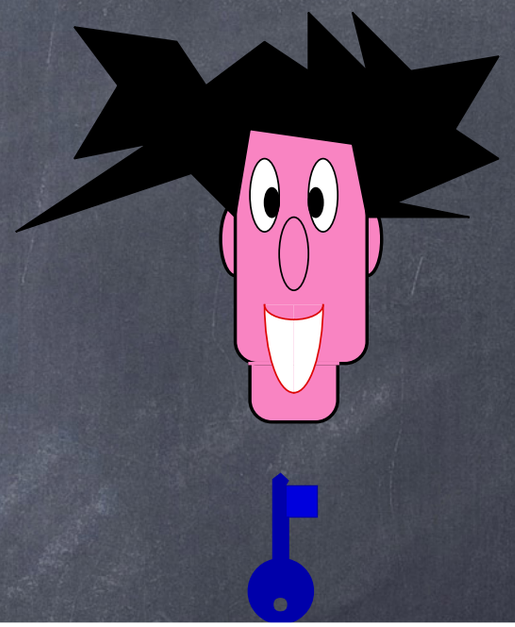


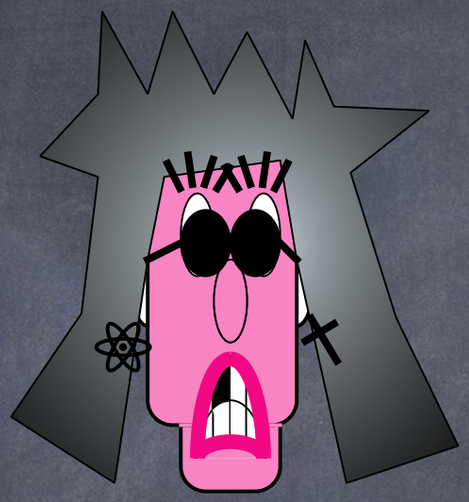
Encryption

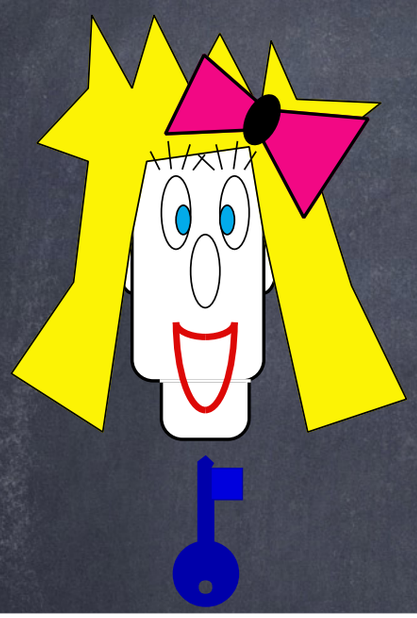




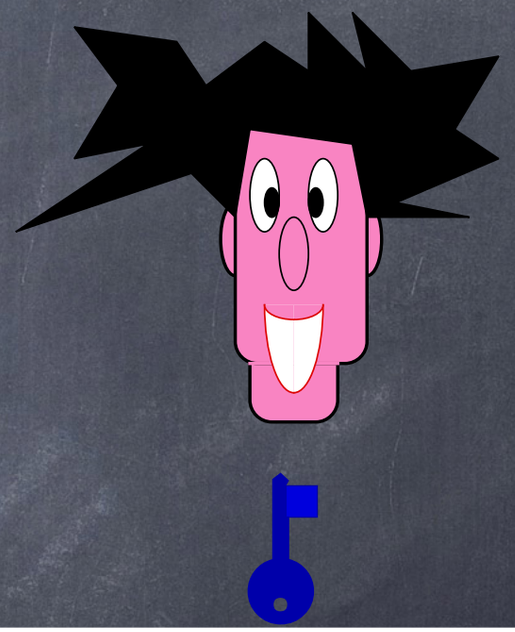
8RdewtU5qkLa$es!T9@





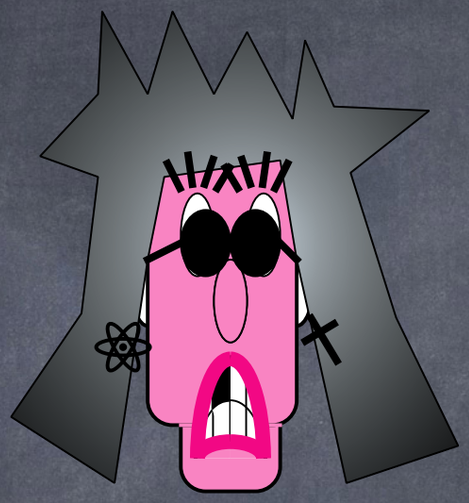


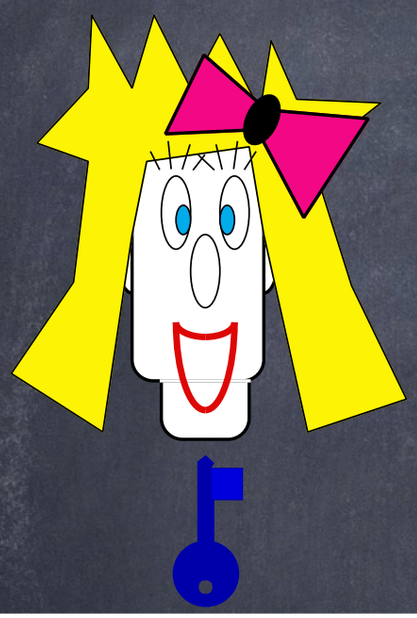
8RdewtU5qkLa$es!T9@



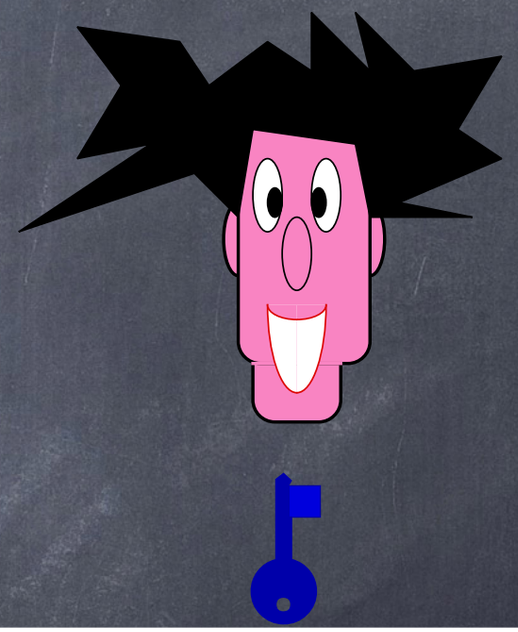
Encryption

8RdewtU5qkLa9 y me ?





8RdewtU5qkLa$es!T9@

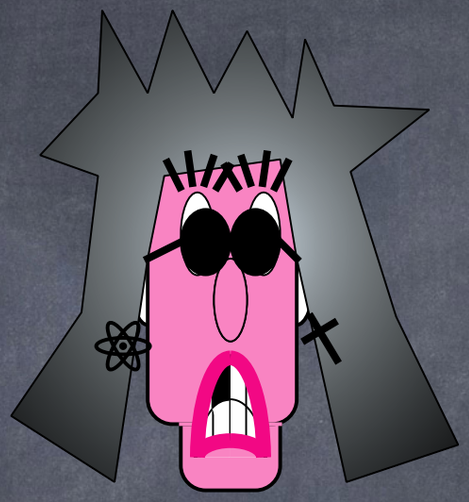


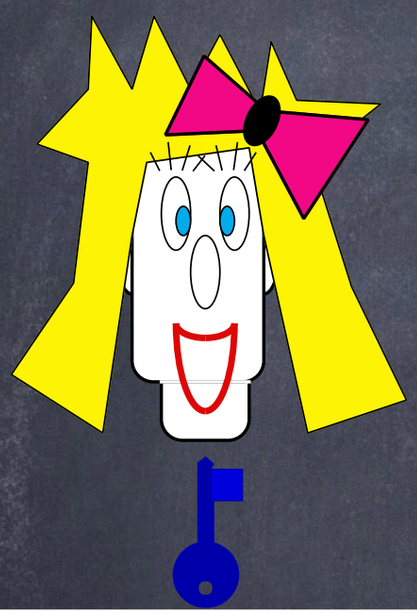
Decryption

Will you marry m es!T9@

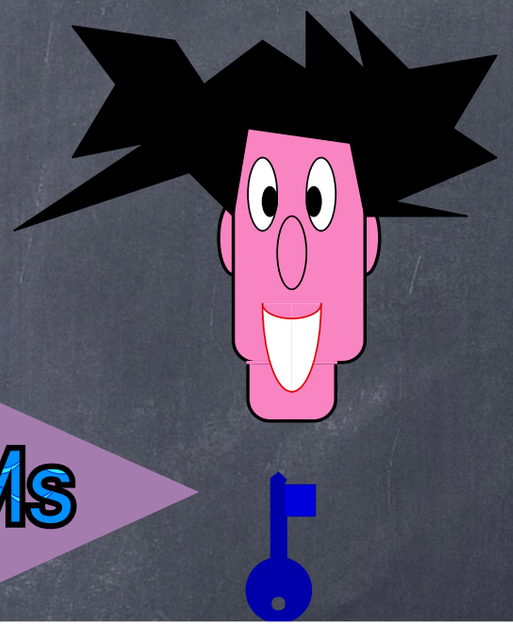
Encryption

8RdewtU5qkLa9 y me ?

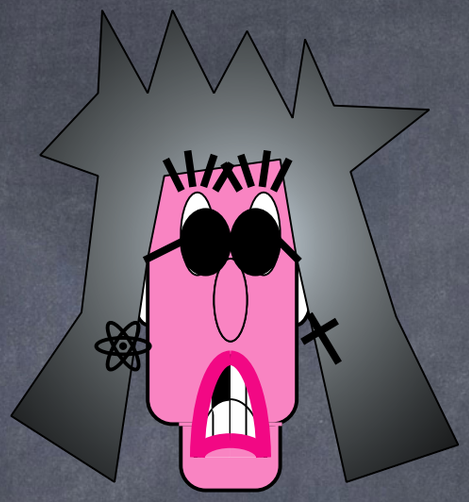


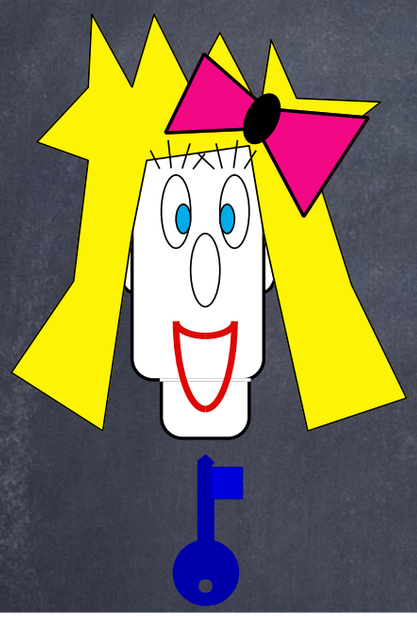


8RdewtU5qkLa$es!T9@

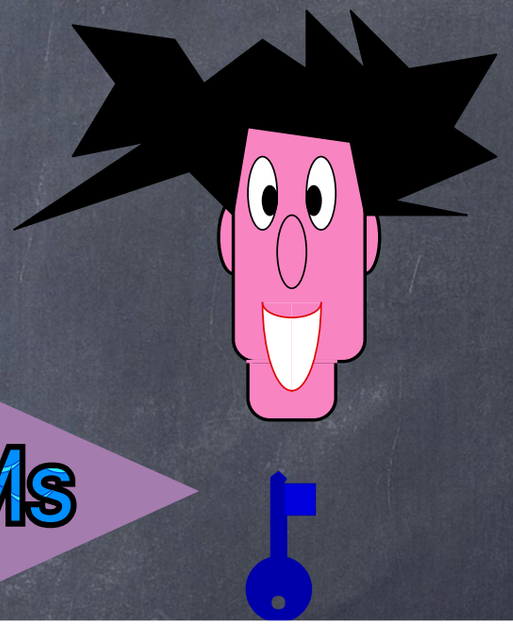


I(D%eXhDqIiykI#2cV7dEwnMs





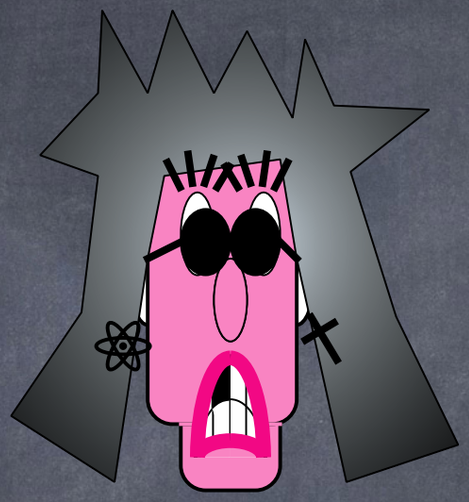
8RdewtU5qkLa$es!T9@

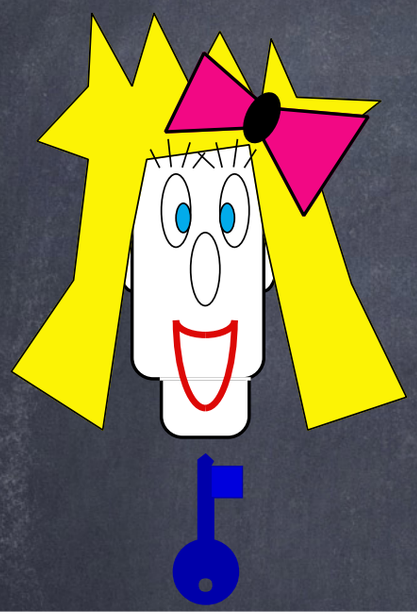


I(D%eXhDqIiykI#2cV7dEwnMs

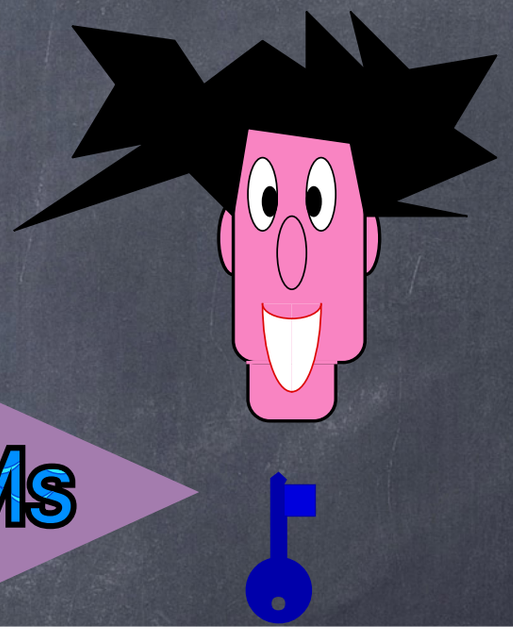
Encryption

Divorce your wif 2cV7dEwnMs





8RdewtU5qkLa$es!T9@



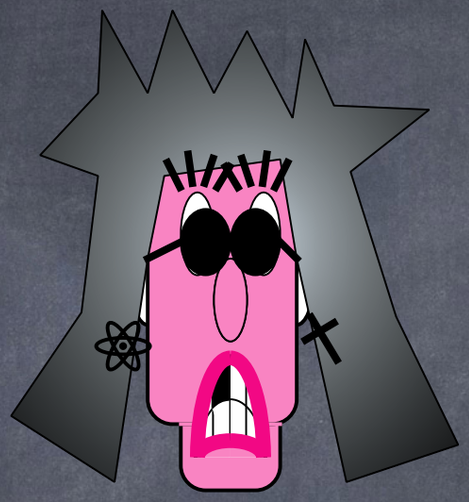
I(D%eXhDqIiykI#2cV7dEwnMs

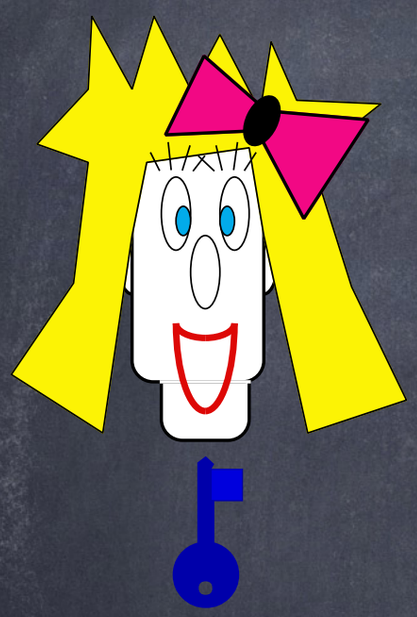
Encryption

Divorce your wif 2cV7dEwnMs

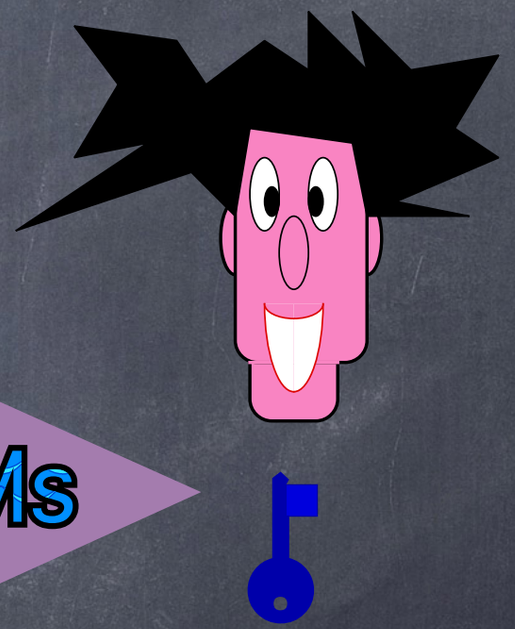
Decryption

I(D%eXhDqIiykI#2cV7 ur wife first !



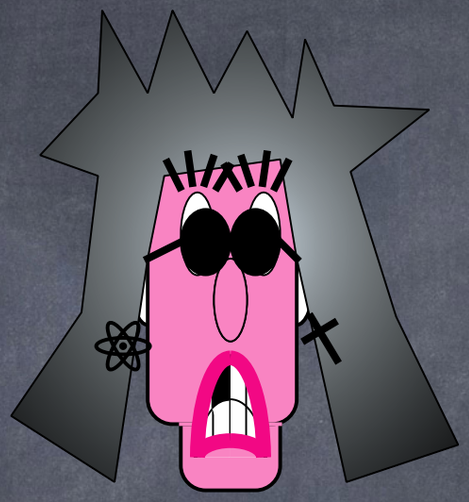


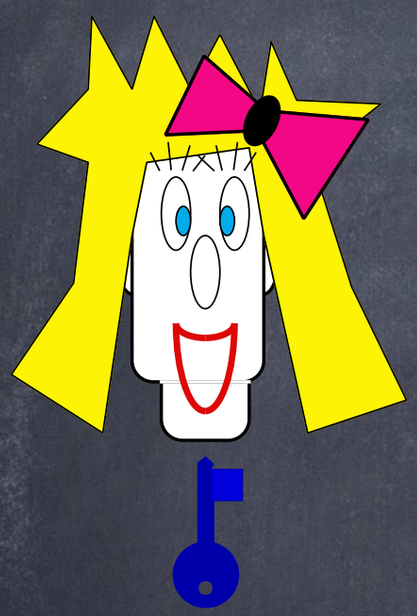
8RdewtU5qkLa$es!T9@



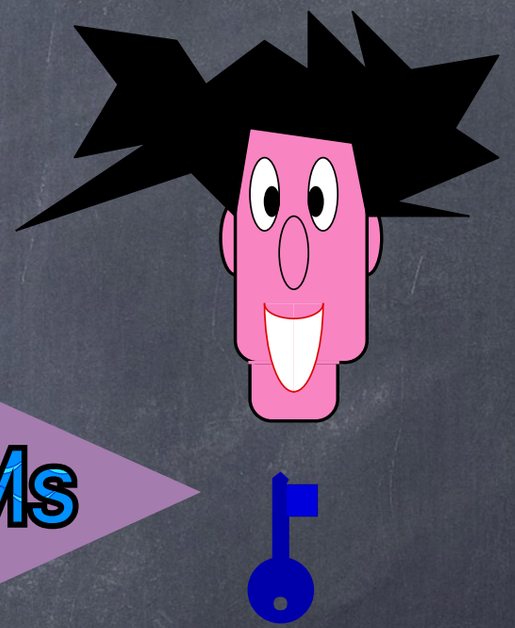
I(D%eXhDqIiykI#2cV7dEwnMs

H&fs@tyHvFGhaOKpTrGbI.Z/rUih*





8RdewtU5qkLa$es!T9@

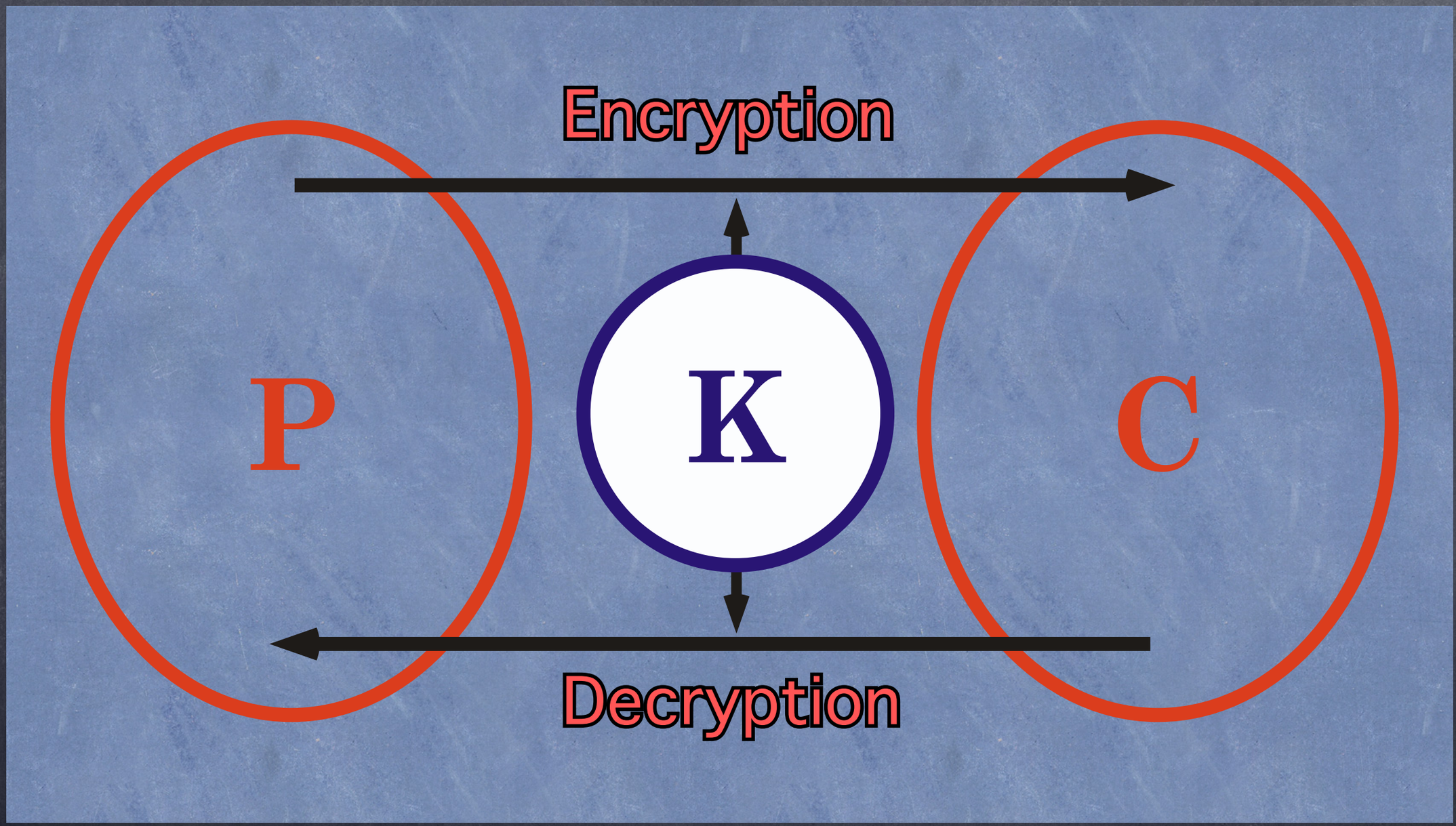


l(D%eXhDqIiykI#2cV7dEwnMs

H&fs@tyHvFGhaOKpTrGbI.Z/rUih*

B7B3tdsjUila

Symmetric Encryption



Information Theoretical Security

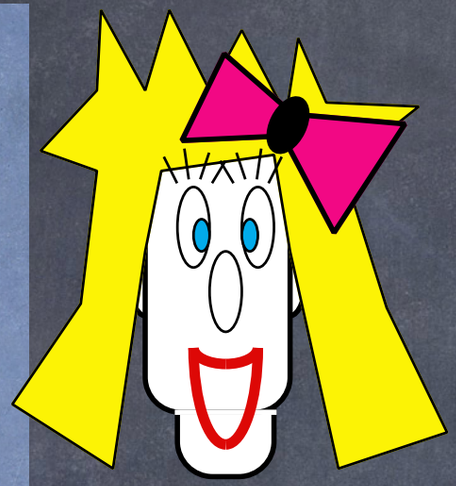
Symmetric Encryption

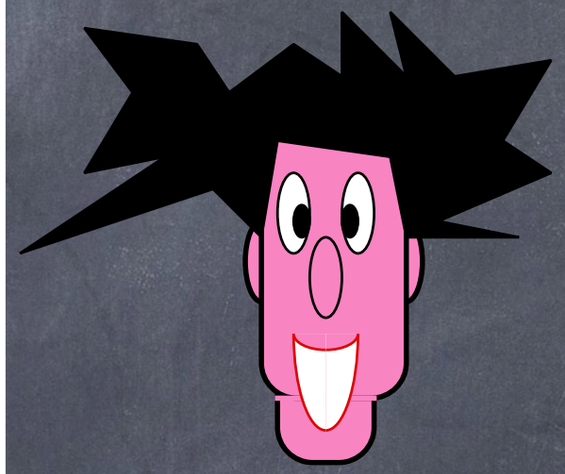
Ceasar's Cipher

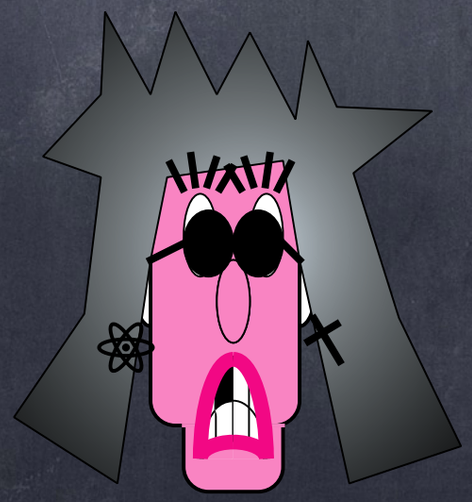
VERNAM's Cipher

m

1
0
1
0
0
1
0
0
1
1
1
1
1
1
0
0
1

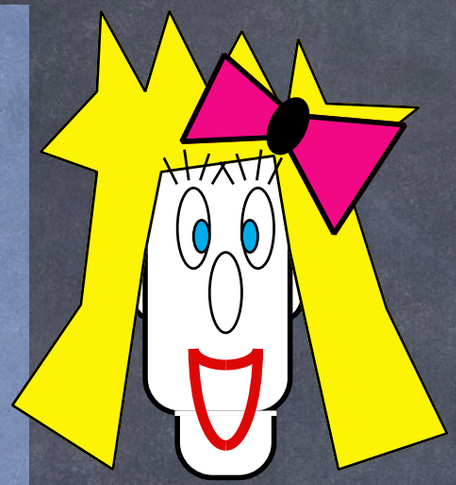


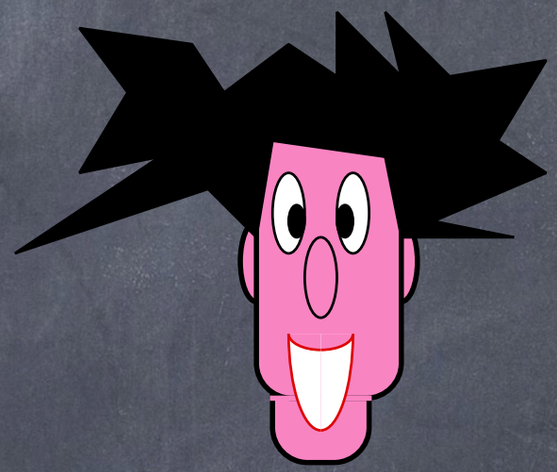


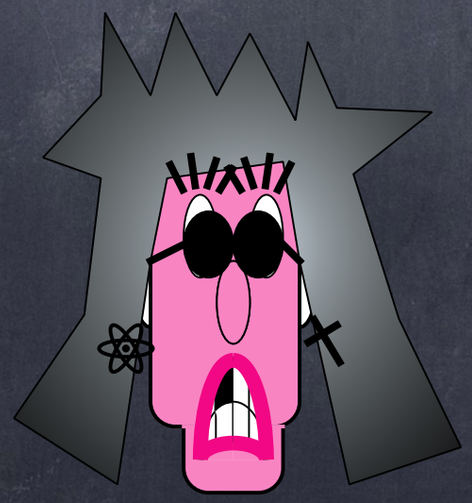


VERNAM's Cipher

m	⊕	k
1		1
0		1
1		1
0		0
0		0
1		1
0		1
0		0
1		1
1		1
1		0
1		1
1		0
0		1
0		1
1		1

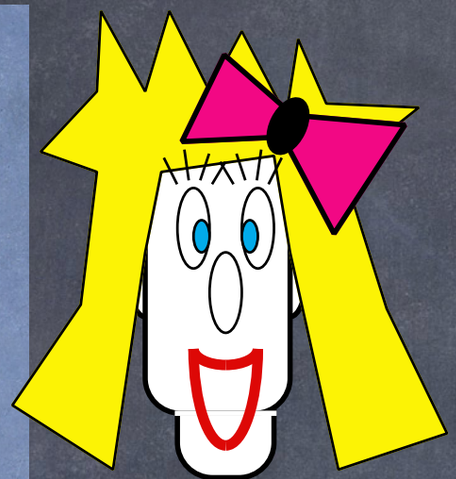


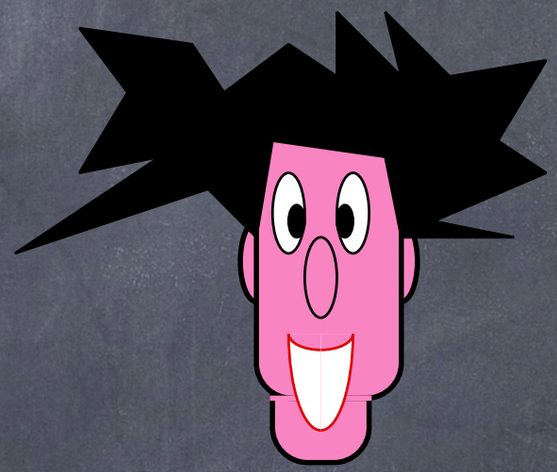


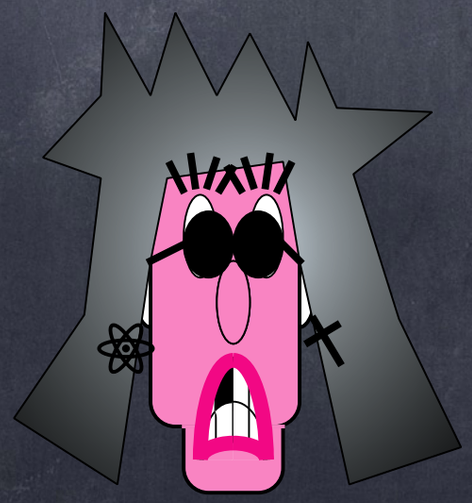


VERNAM's Cipher

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

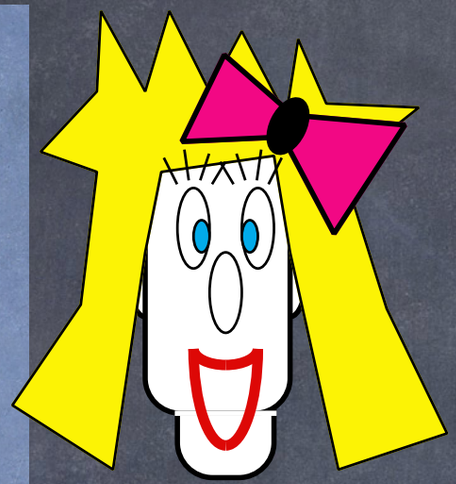


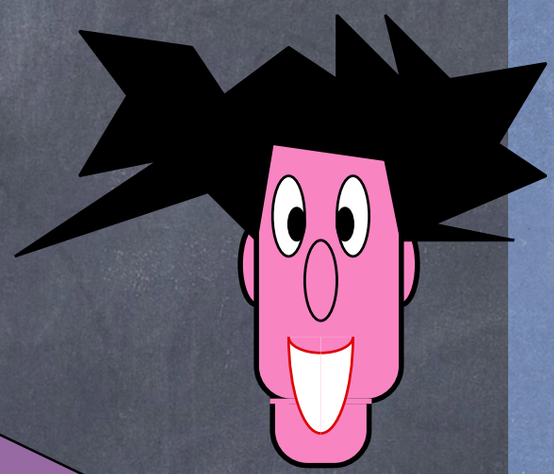




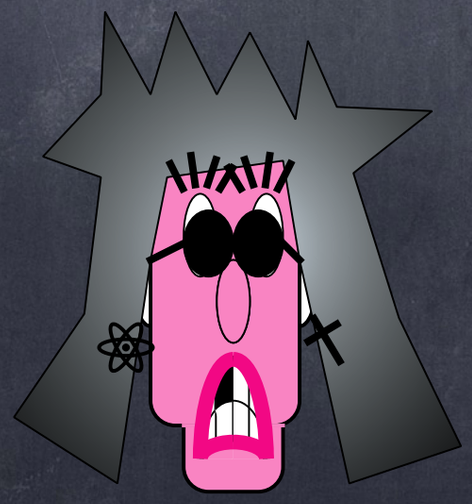
VERNAM's Cipher

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





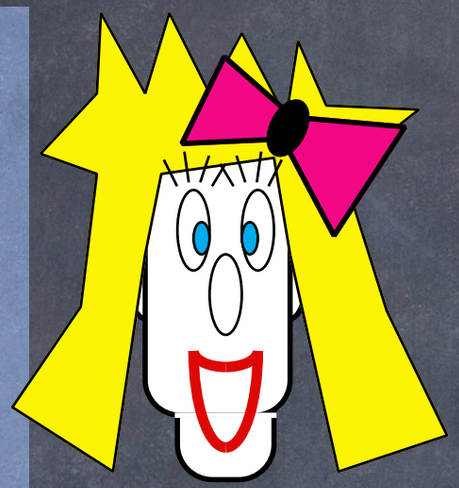
c

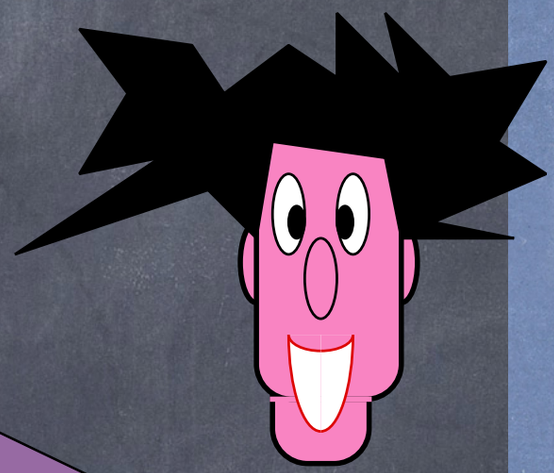


c
0
1
0
0
0
0
0
1
0
0
0
0
1
0
1
1
1
0

VERNAM's Cipher

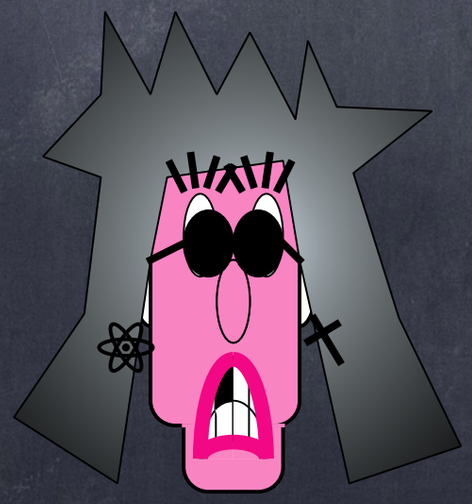
m	⊕	k	=	c
1		1		0
0		1		1
1		1		0
0		0		0
0		0		0
1		1		0
0		1		1
0		0		0
1		1		0
1		0		1
1		1		0
1		0		1
0		1		1
0		1		1
1		1		0





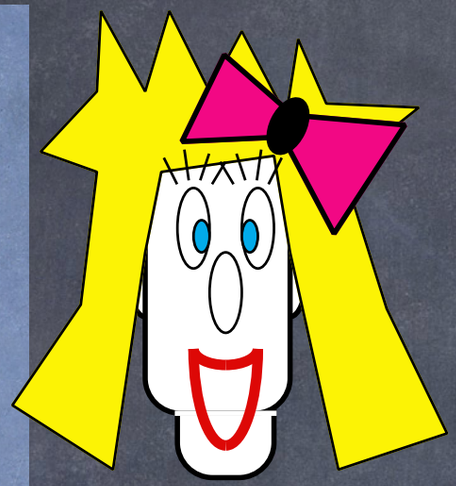
c

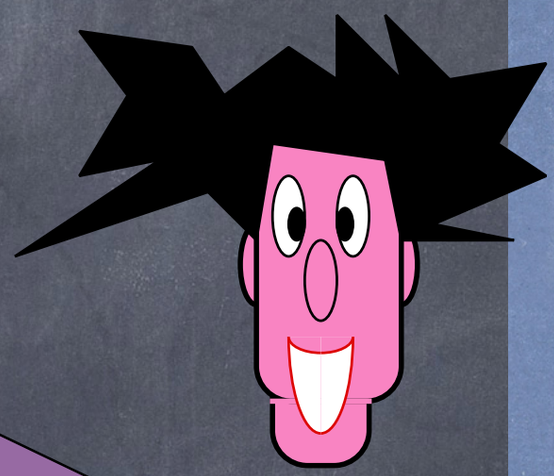
c	⊕	k
0		1
1		1
0		1
0		0
0		0
0		1
0		1
1		0
0		1
1		0
1		1
1		1
0		1



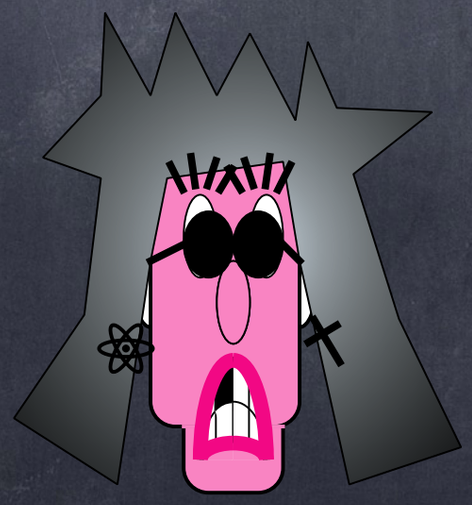
VERNAM's Cipher

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		0		1
1		1		0
1		0		1
0		1		1
0		1		1
1		1		0





c



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
1		0		1
0		1		1
1		0		1
1		1		0
1		1		0
0		1		1

VALKIA VI

[redacted]

[redacted]

[redacted]

[illegible]

[redacted]

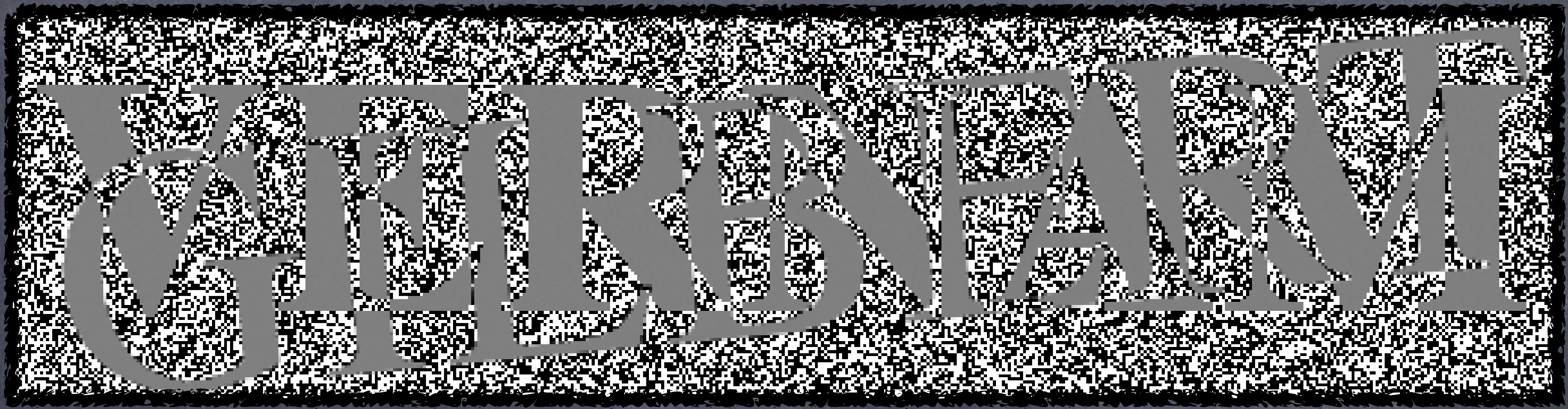
[redacted]

[redacted]

[redacted]

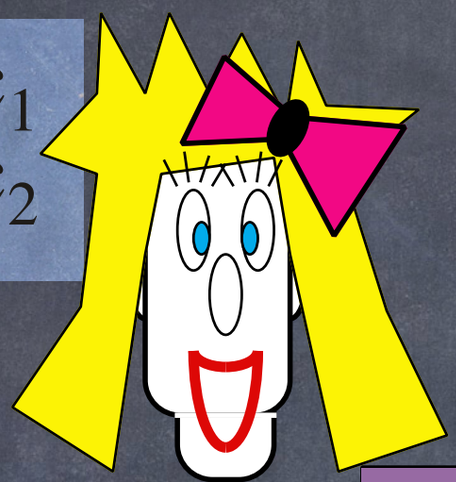
[redacted]

[redacted]



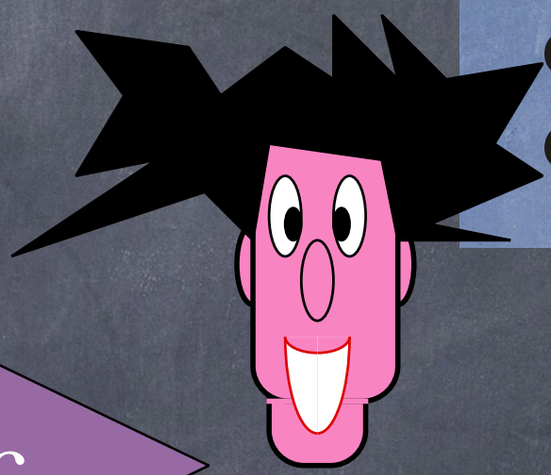
VERNAM's One-Time Pad

$m_1 \oplus k = c_1$
$m_2 \oplus k = c_2$

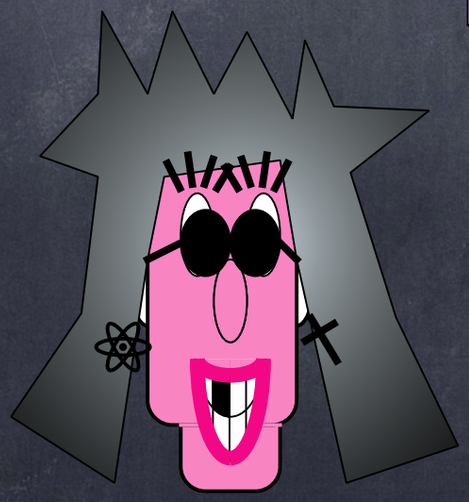


c_1

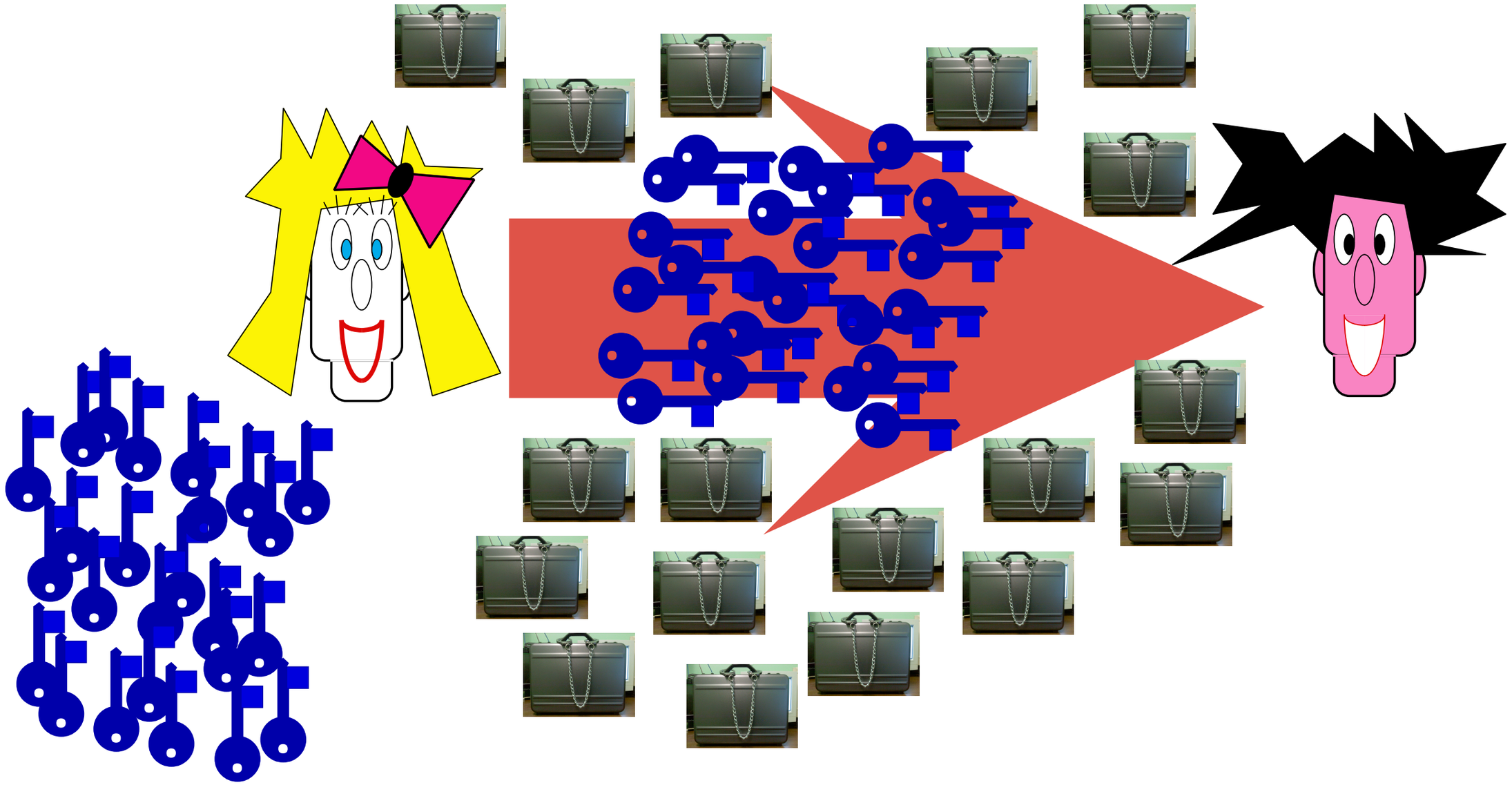
c_2



$c_1 \oplus k = m_1$
$c_2 \oplus k = m_2$

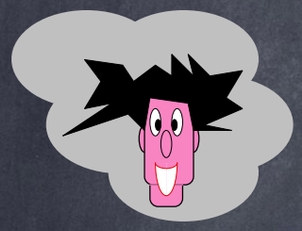


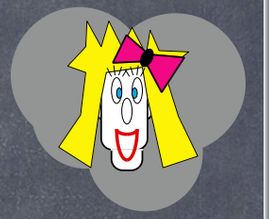
$c_1 \oplus c_2 = m_1 \oplus m_2$

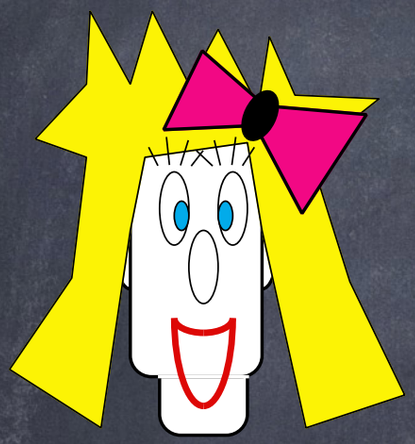


Authentication

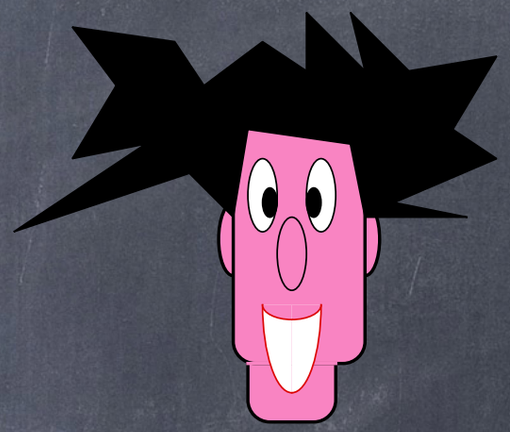
Authentication



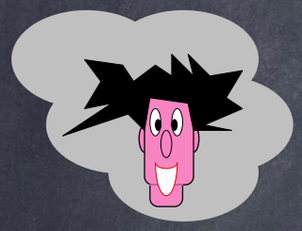


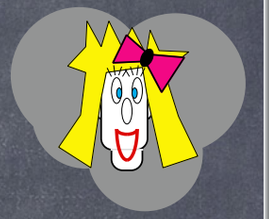


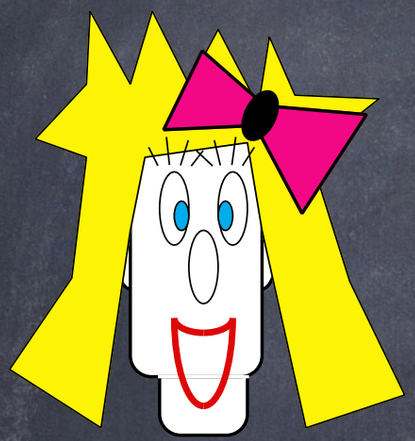
Will you marry me ?



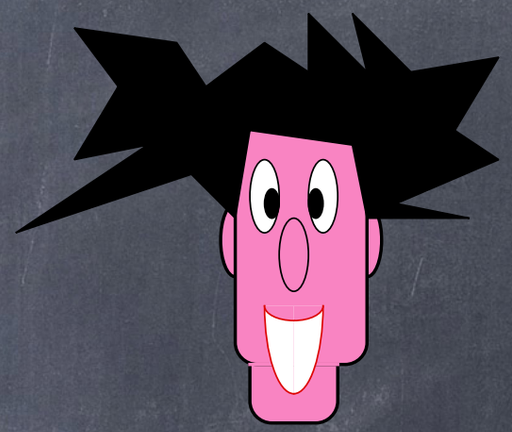
Authentication



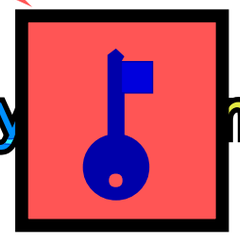




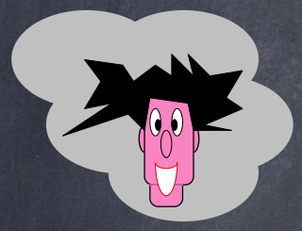
Will you marry me ?

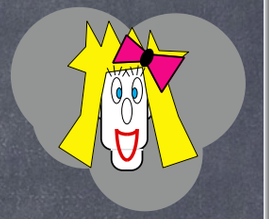


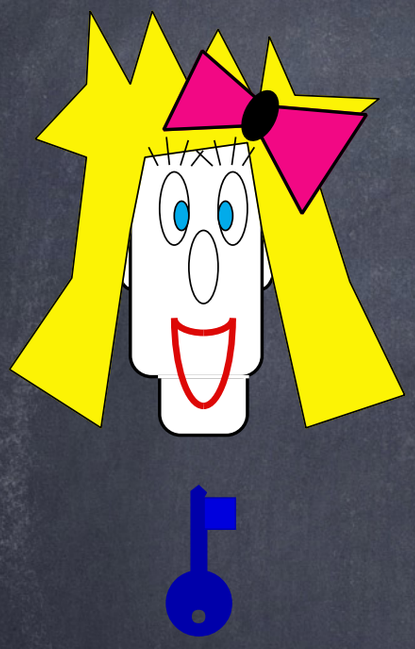
Authentication

Will you marry  me ?

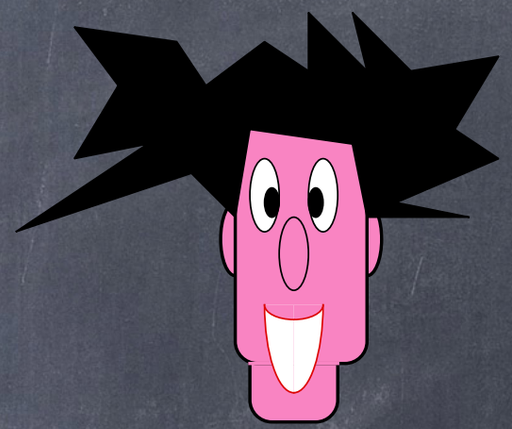
Authentication



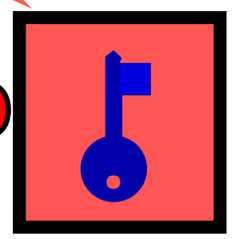




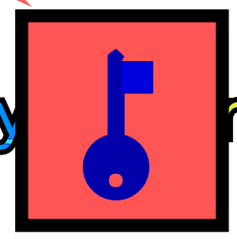
Will you marry me ?



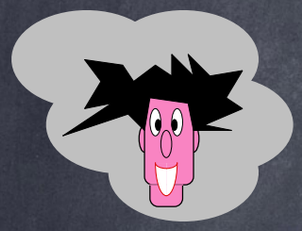
Verification

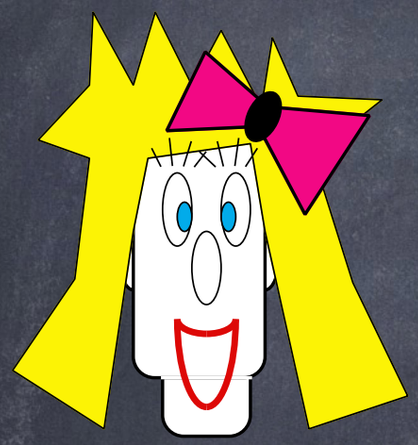
VALID  marry me ?

Authentication

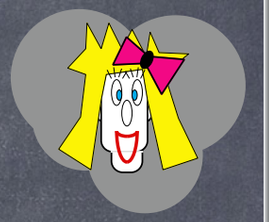
Will you marry  me ?

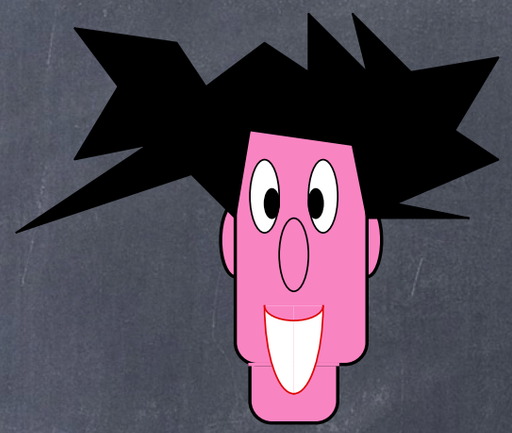
Authentication





Will you marry me ?



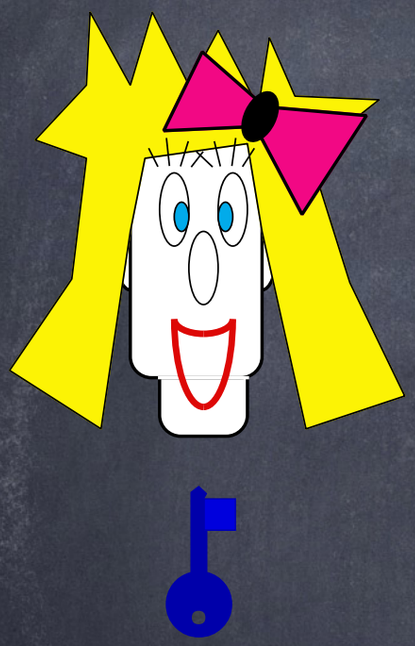


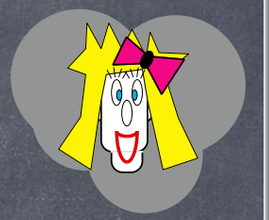
Divorce your wife first !

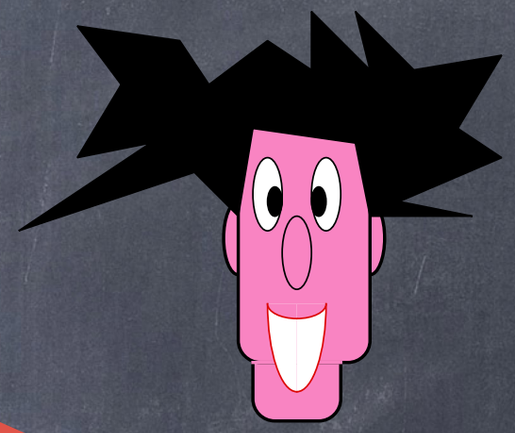
The papers are in the mail...

OK, I will !

Symmetric Authentication

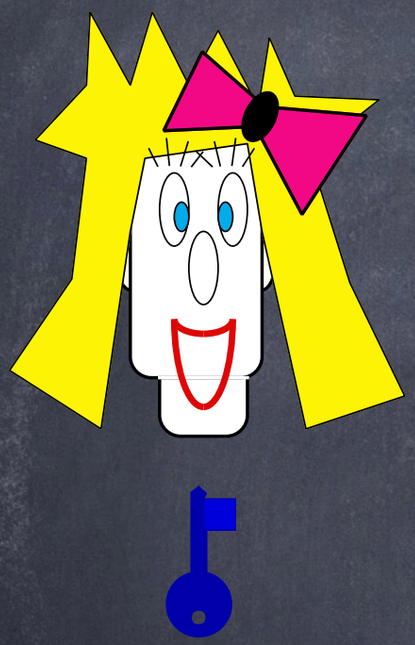


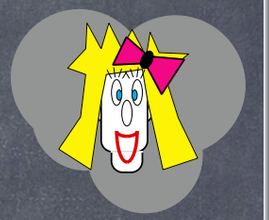


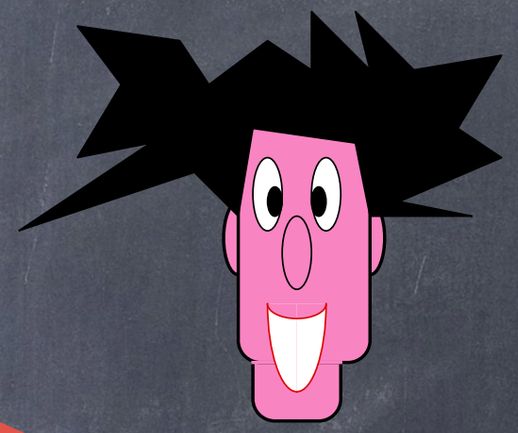


(m,t)

Symmetric Authentication





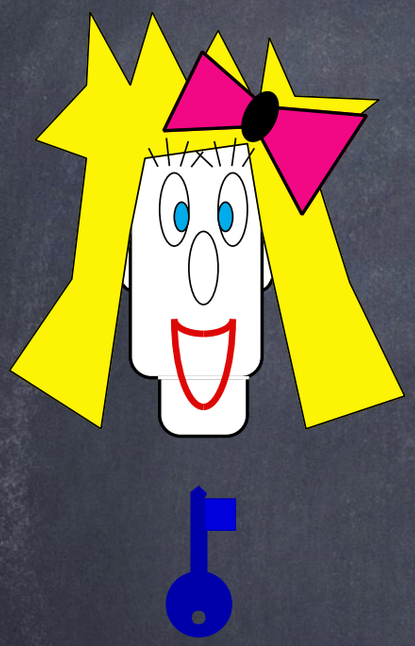


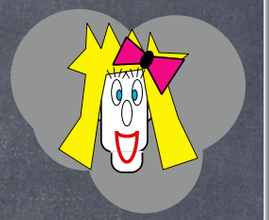
(m,t)

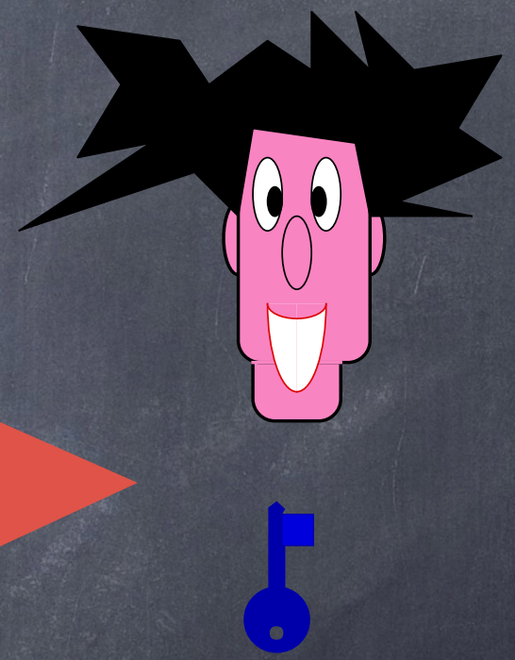
Authentication

$t := A_k(m)$

Symmetric Authentication







(m,t)

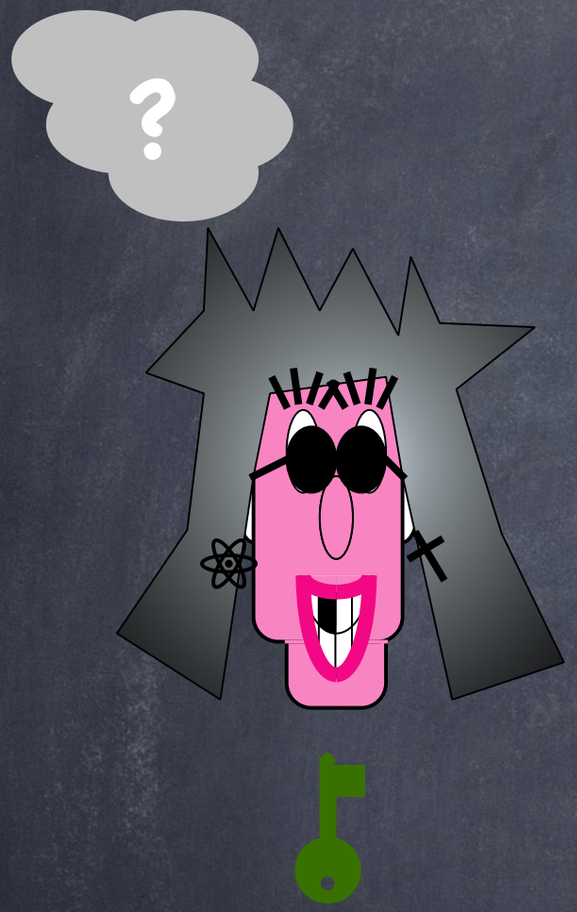
Authentication

$t := A_k(m)$

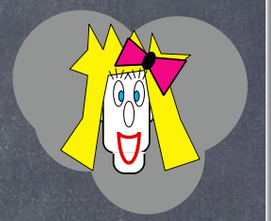
Verification

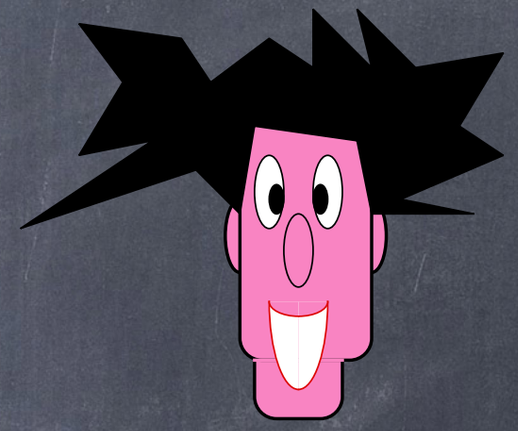
$t = A_k(m)$?

Authentication

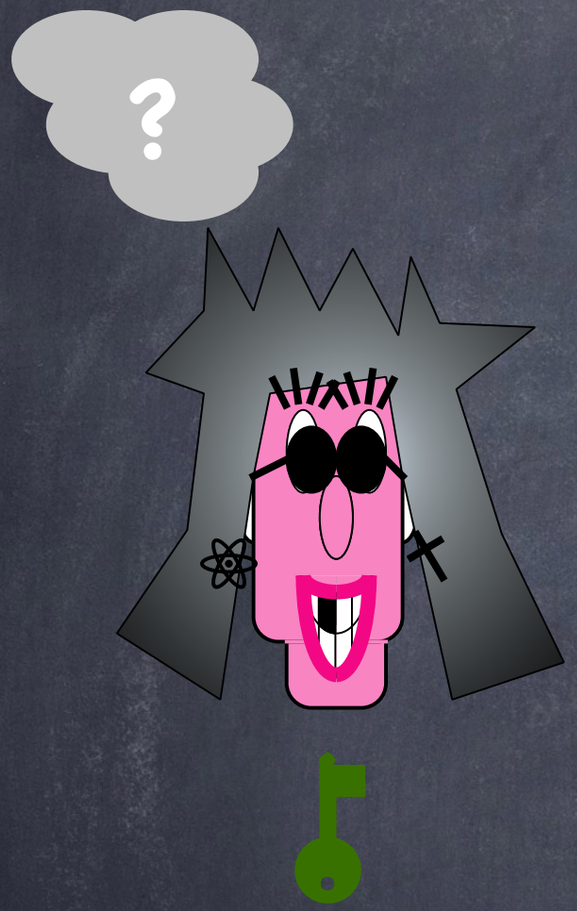


Will you marry me ?

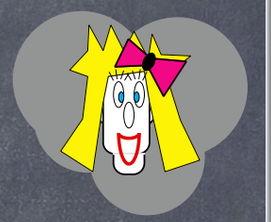


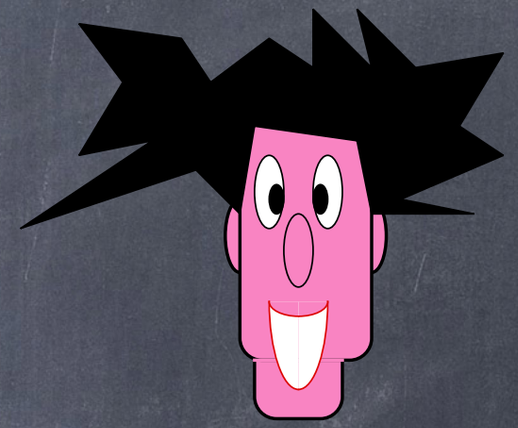


Authentication

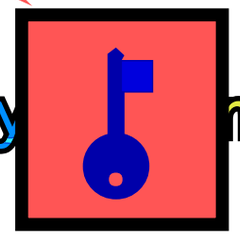


Will you marry me ?

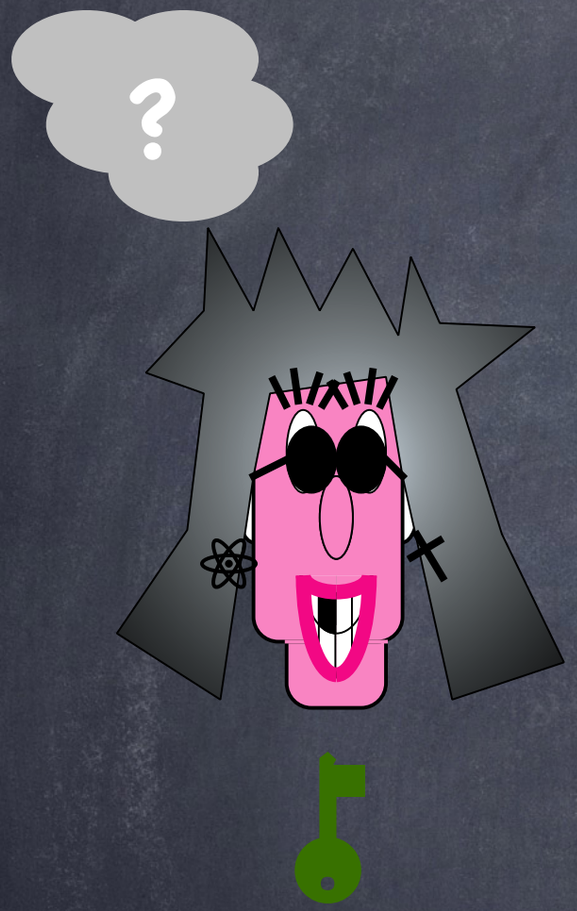




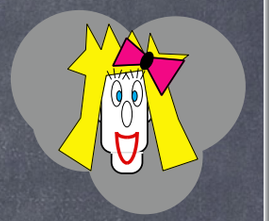
Authentication

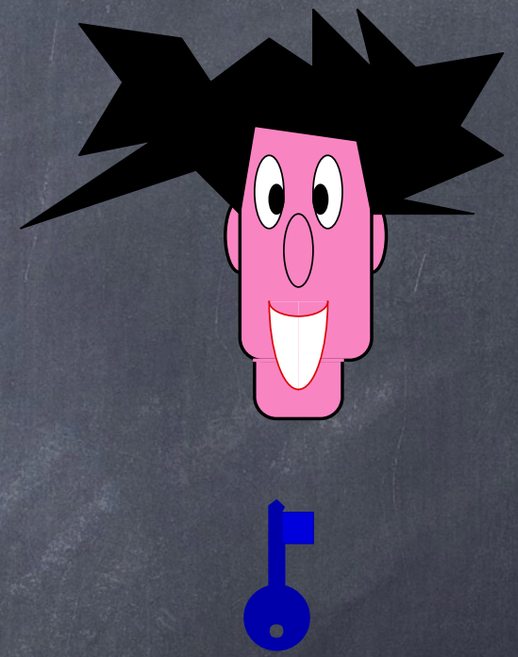
Will you marry  me ?

Authentication

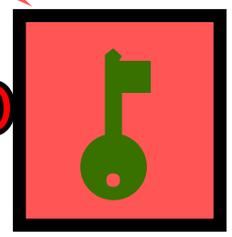


Will you marry me ?

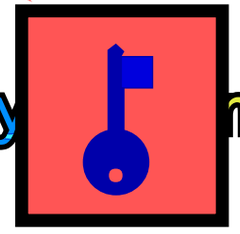




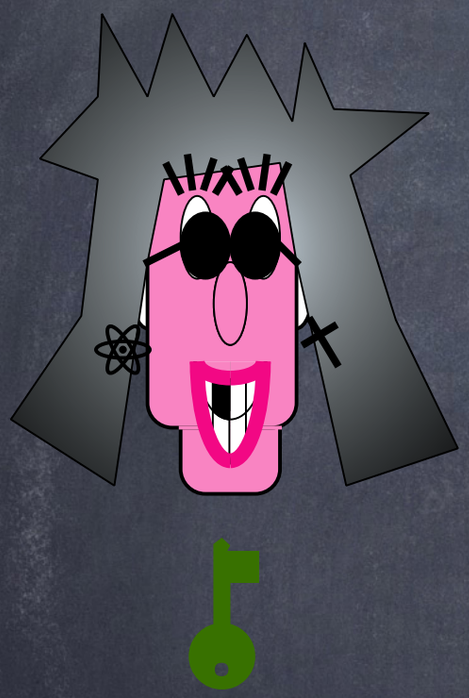
Verification

INVALID  marry me ?

Authentication

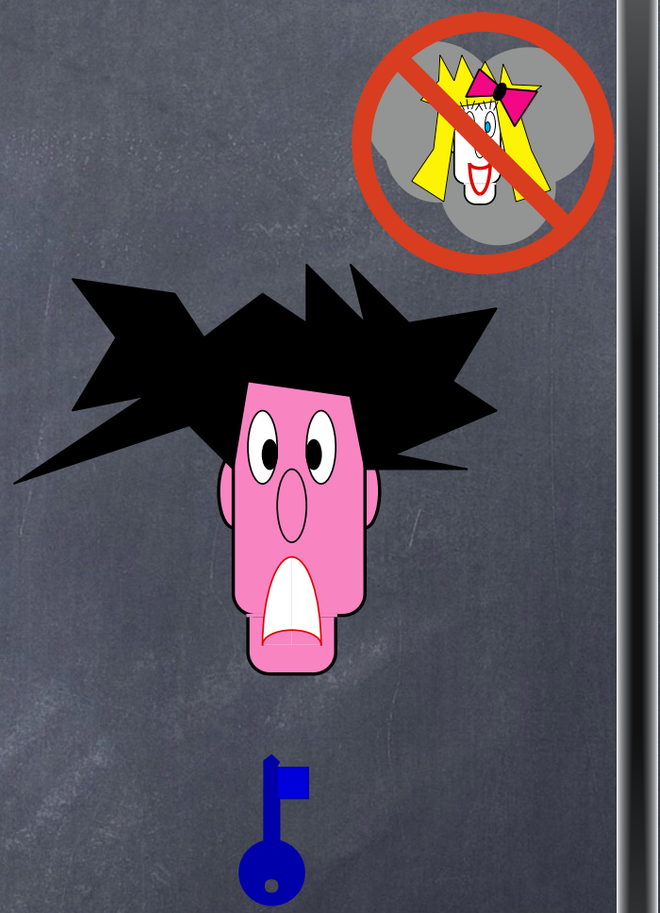
Will you marry  me ?

Authentication

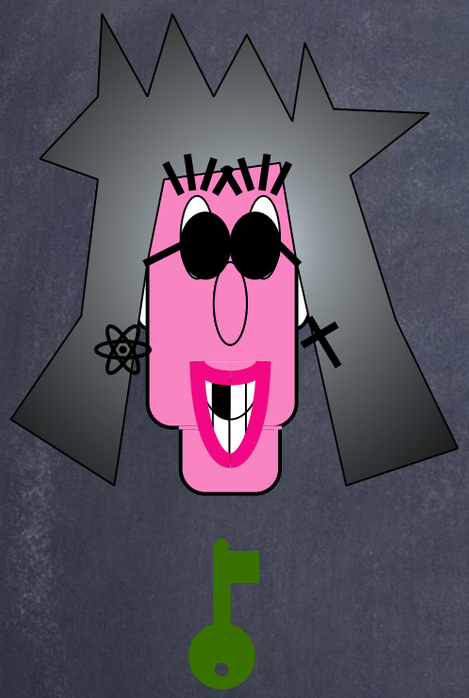


Will you marry me ?

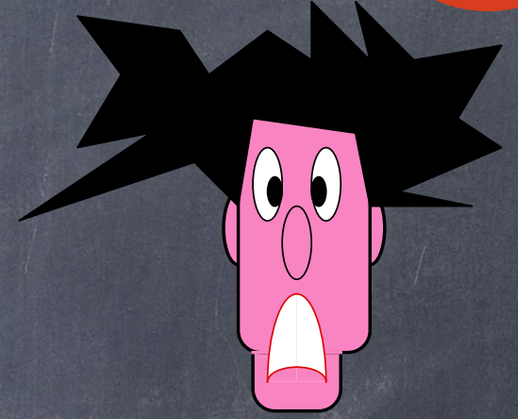
No, I never will !



Authentication

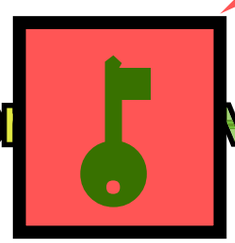


Will you marry me ?



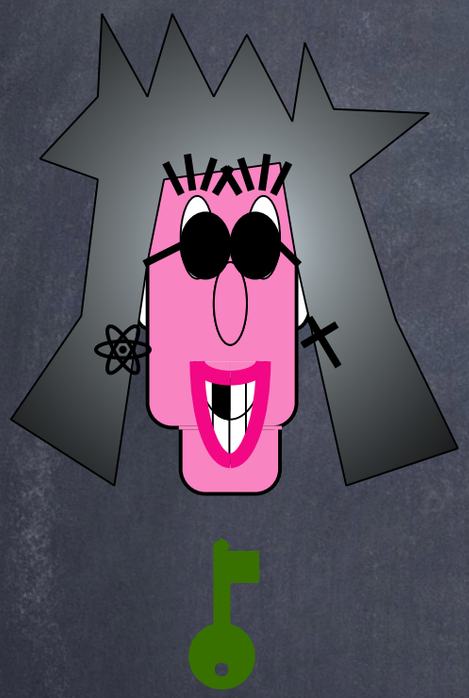
No, I never will !

Authentication



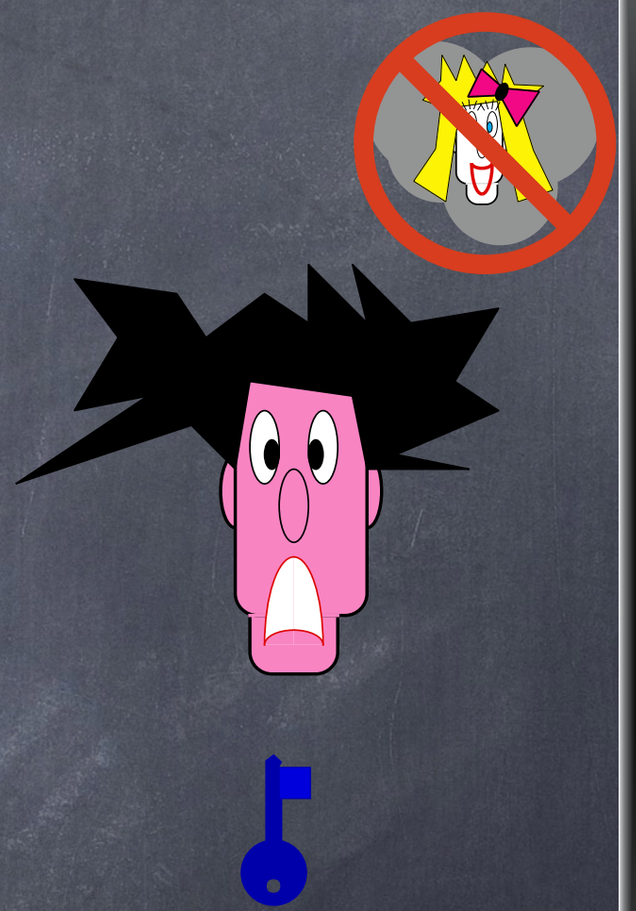
No, I never will !

Authentication

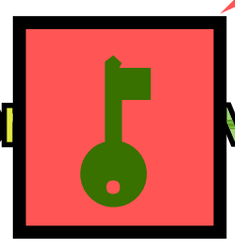


Will you marry me ?

No, I never will !

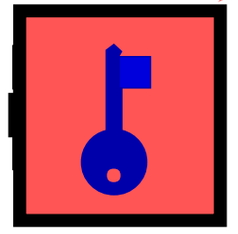


Authentication



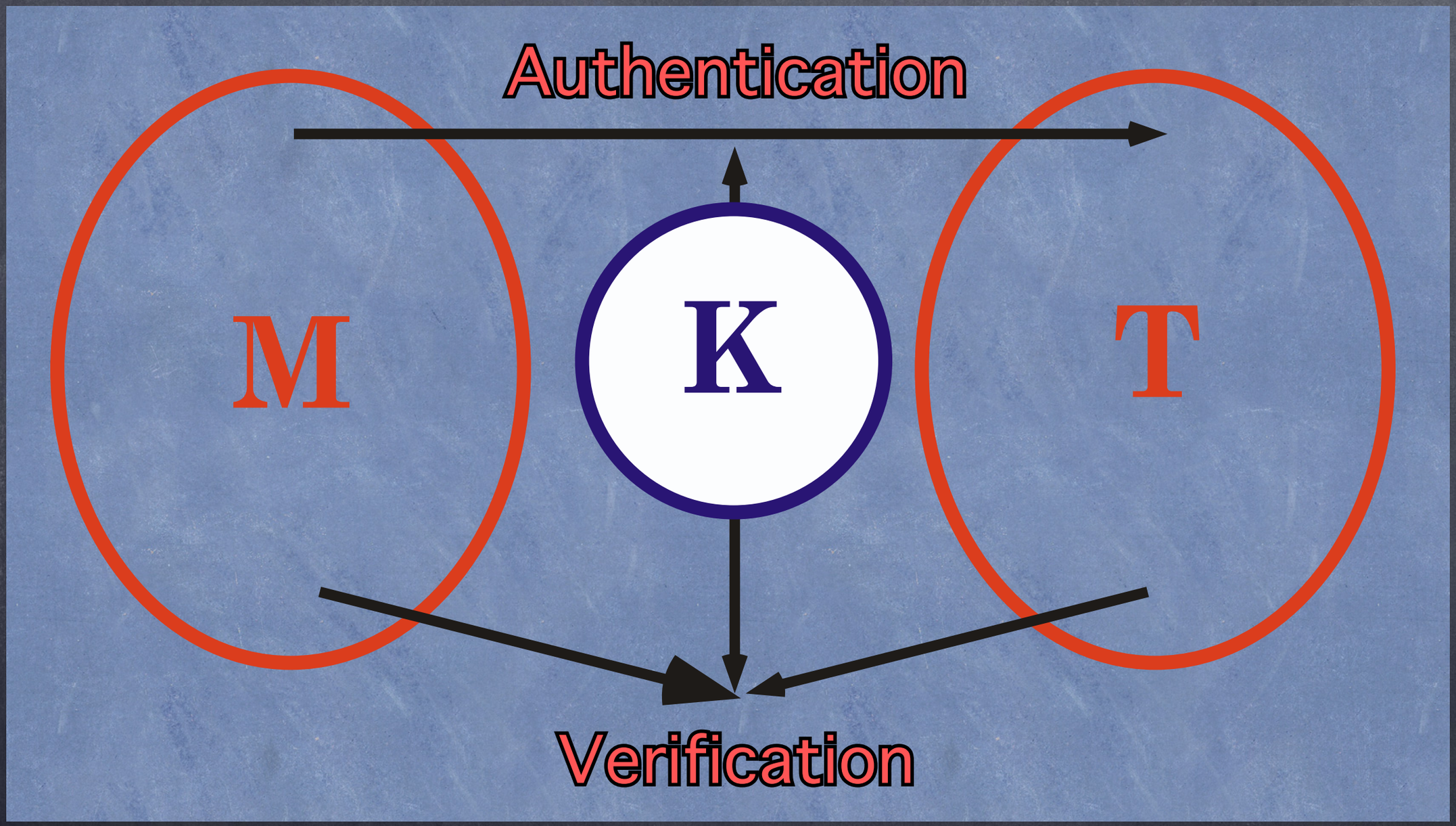
No, I never ever will !

Verification



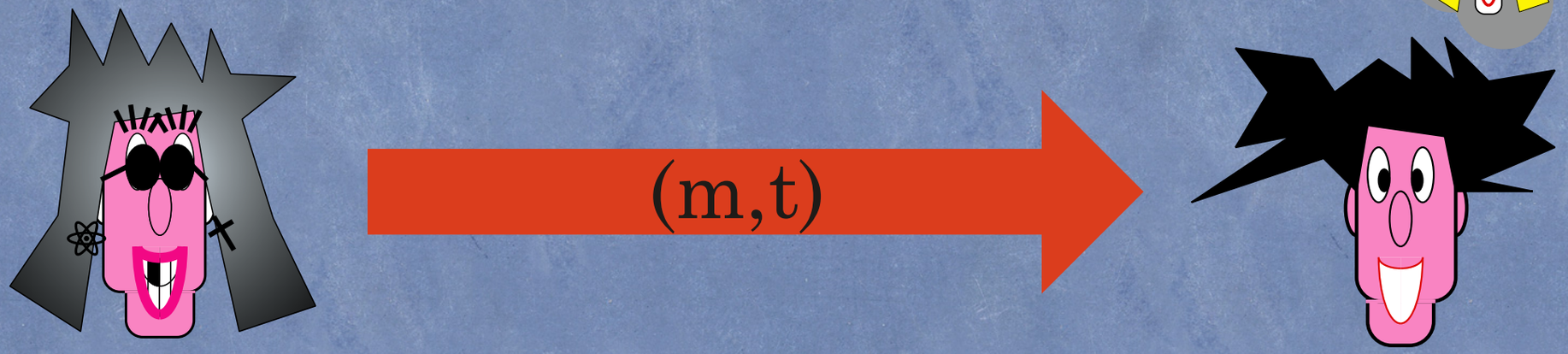
No, I never INVALID

Symmetric Authentication

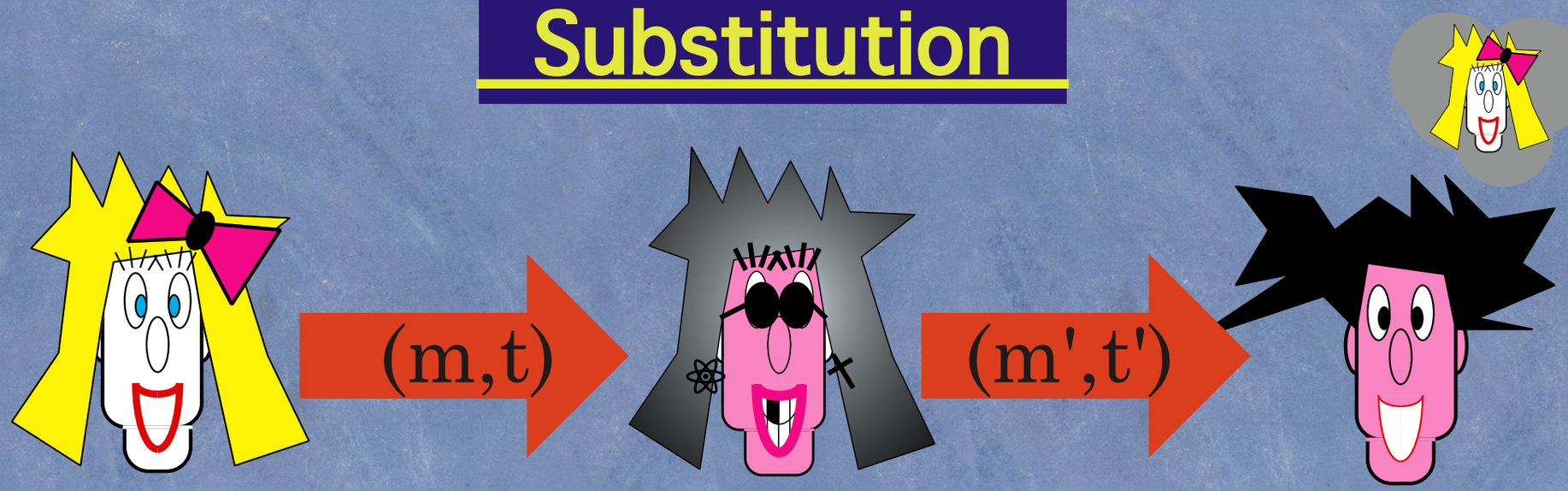


Information Theoretical Security

Impersonation

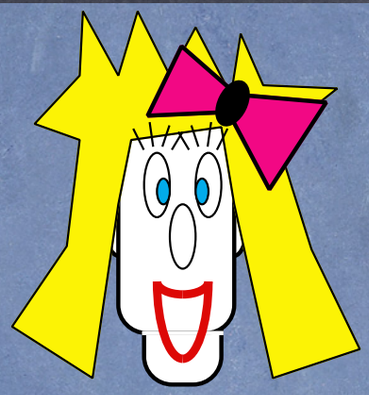


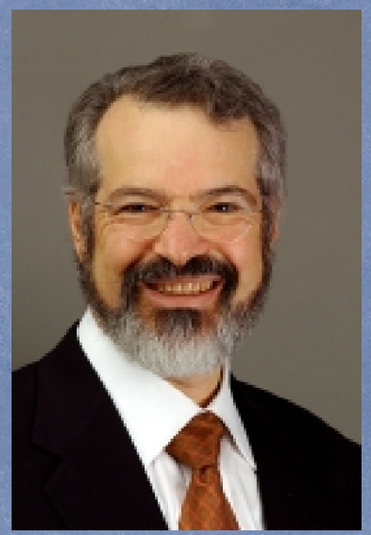
Substitution

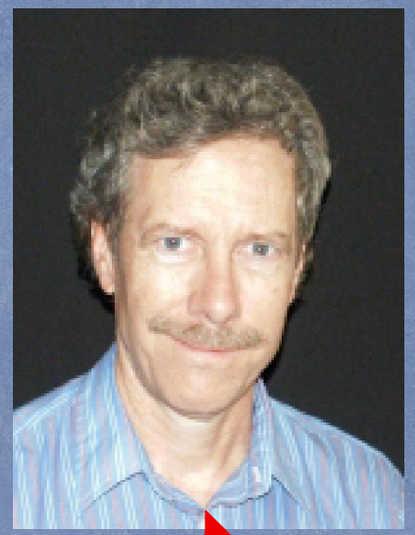


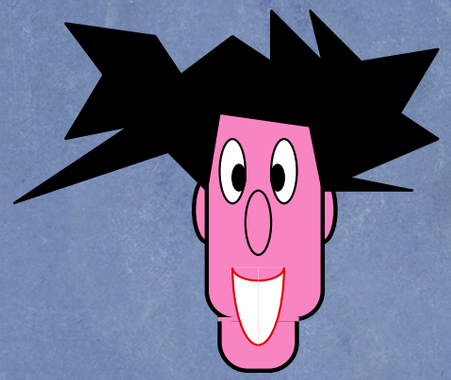
Information Theoretical Security

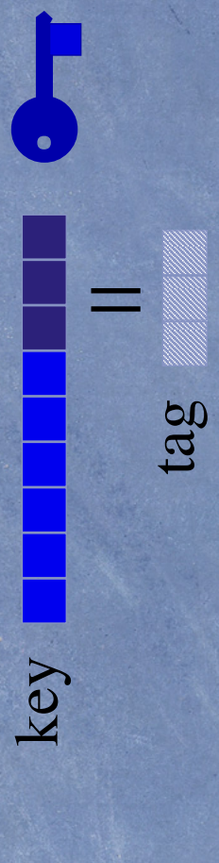
Wegman-Carter One-Time Authentication

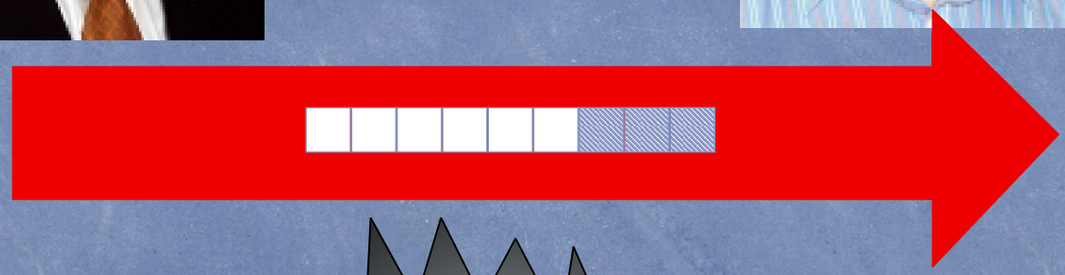


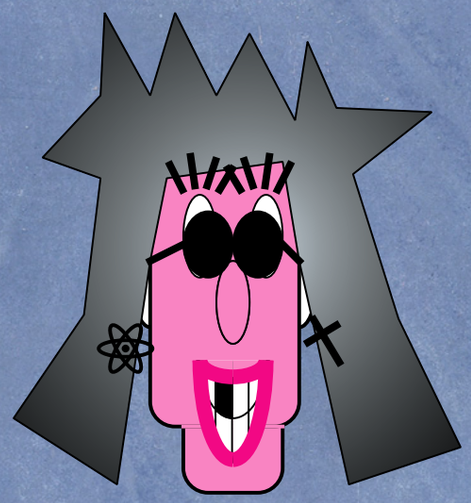


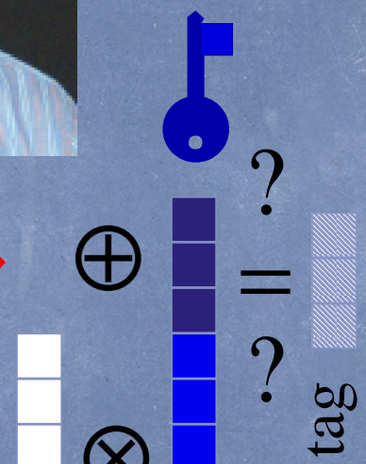




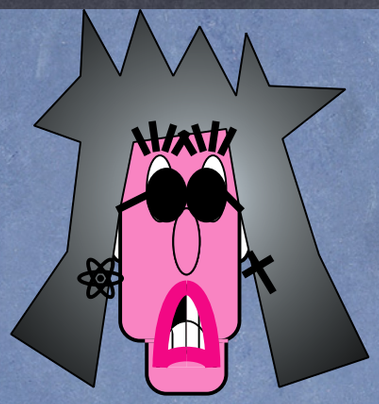


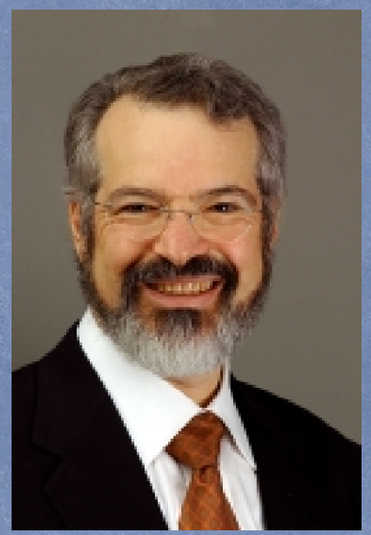


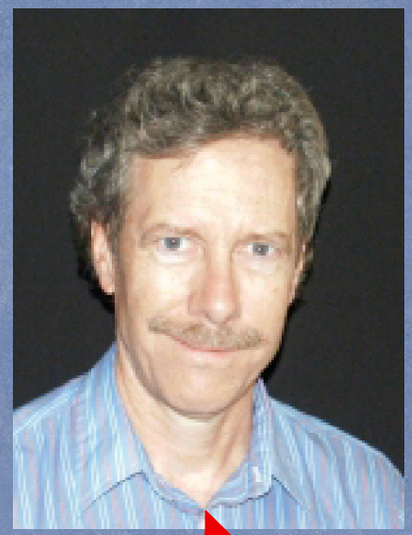


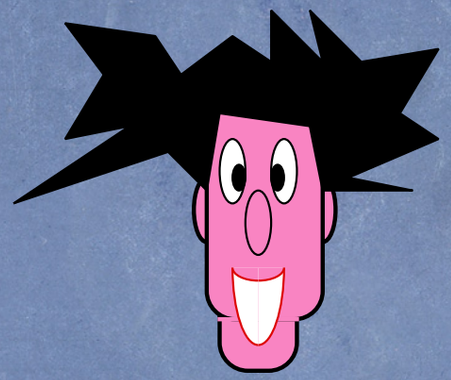


Wegman-Carter One-Time Authentication



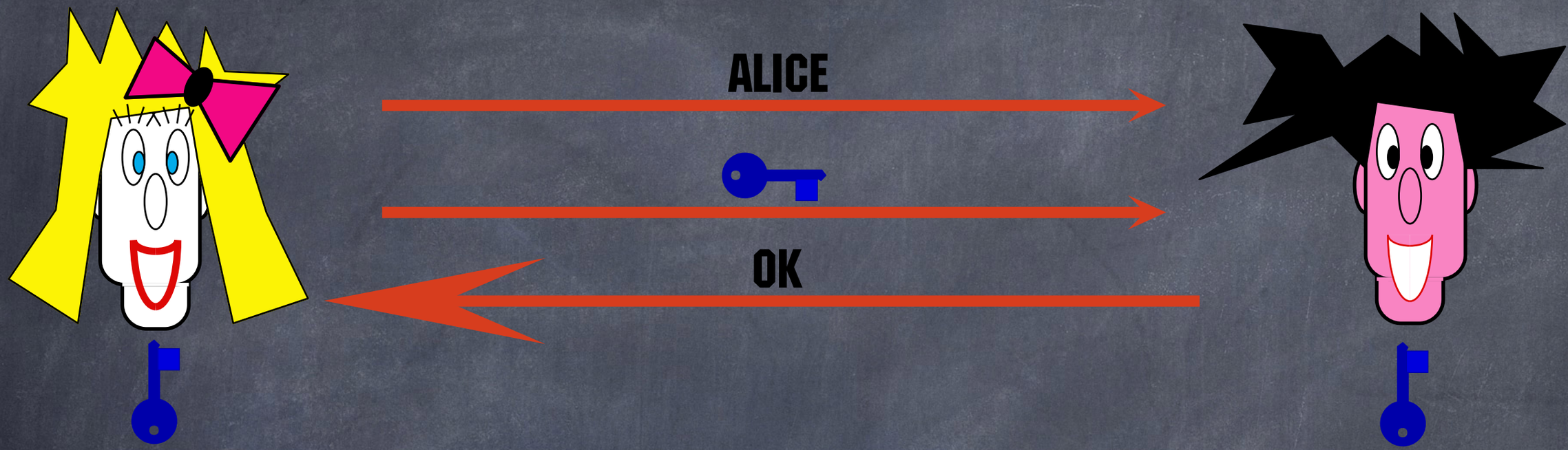






identification

One-Time Identification



MONT-SAINT-HILAIRE

Des fraudeurs déjouent la sécurité des cartes de débit

(Crooks bypass ATM Security)

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

Québec. Il s'agit d'une enquête extrêmement difficile à mener», commente le sergent-détective Bertrand Déry, de la Sécurité publique de Mont-Saint-Hilaire.

JEUNE NOIR RECHERCHÉ

Les informations détenues par les policiers, qui s'apprêtent à déposer des accusations de fraudes contre le commis du dépanneur, indiquent qu'un homme d'une vingtaine d'année, 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.

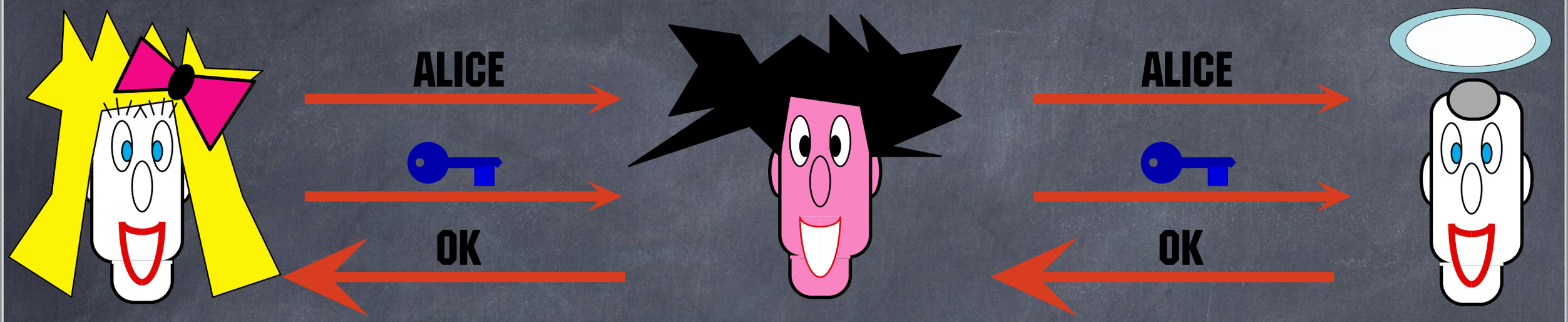
Les policiers sont par ailleurs à la recherche du jeune homme de race noire d'une vingtaine d'années qui se déplace en compagnie de deux complices d'origine liba-

prudences avec les cartes de débit. Et il va même jusqu'à déconseiller leur utilisation. «Nous n'avons aucune idée de l'ampleur de

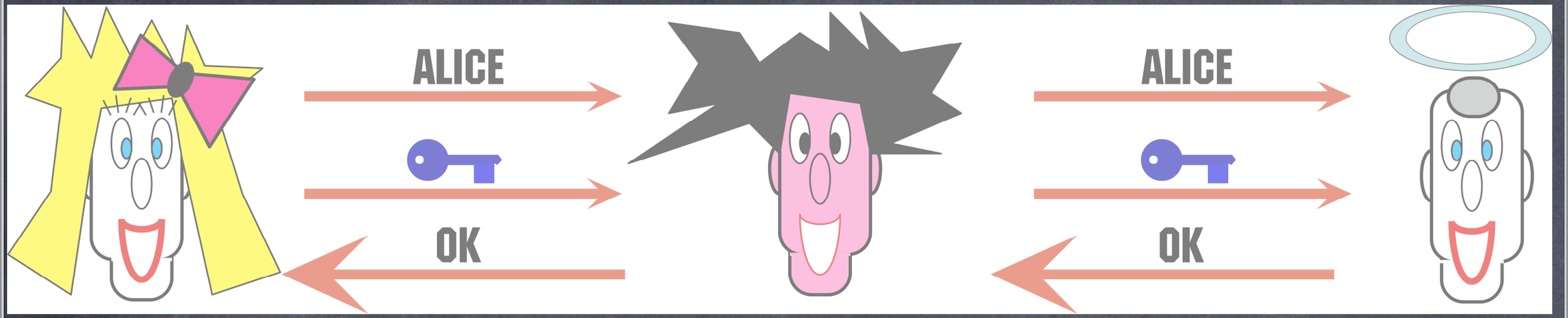
approché par le même fraudeur une semaine plus tôt. Mais il avait refusé de se faire complice», précise M. Déry.

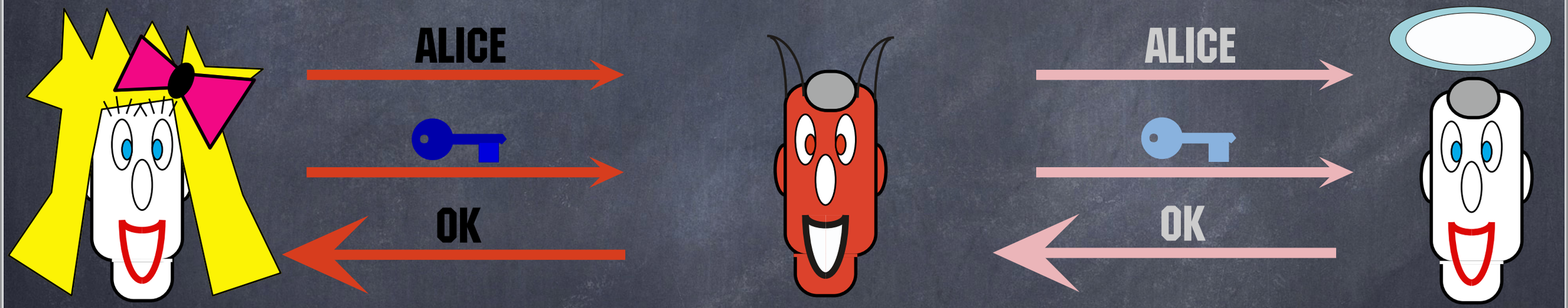
L'individu de race noire qui est recherché par les policiers avait fait une offre à un autre commis d'un dépanneur de Mont-Saint-Hilaire, une semaine avant de commettre ses fraudes.

Impersonation

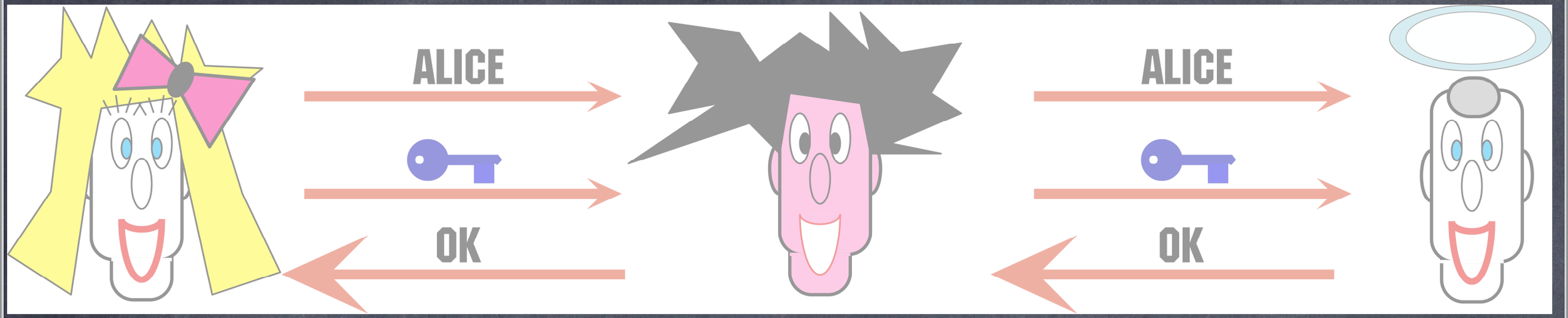


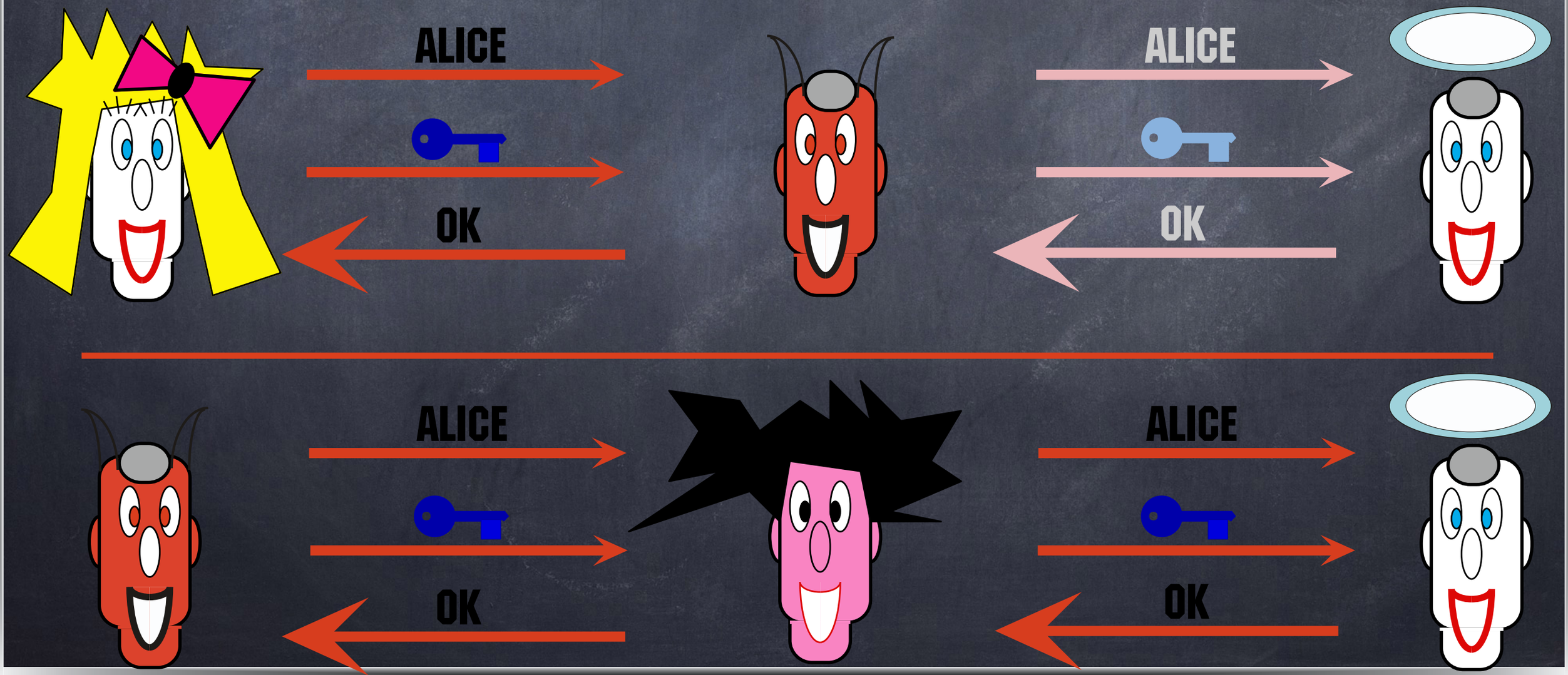
Impersonation



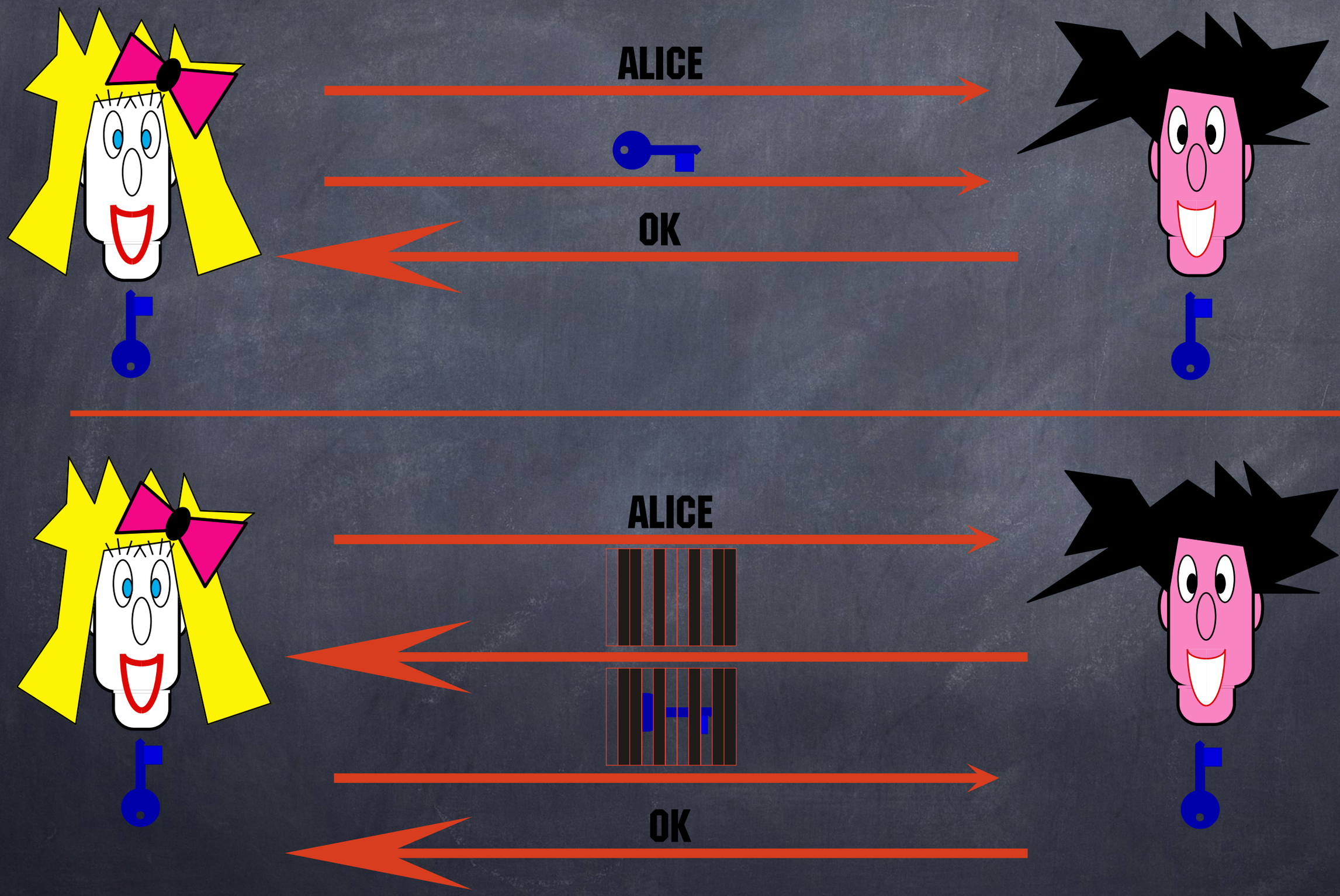


Impersonation





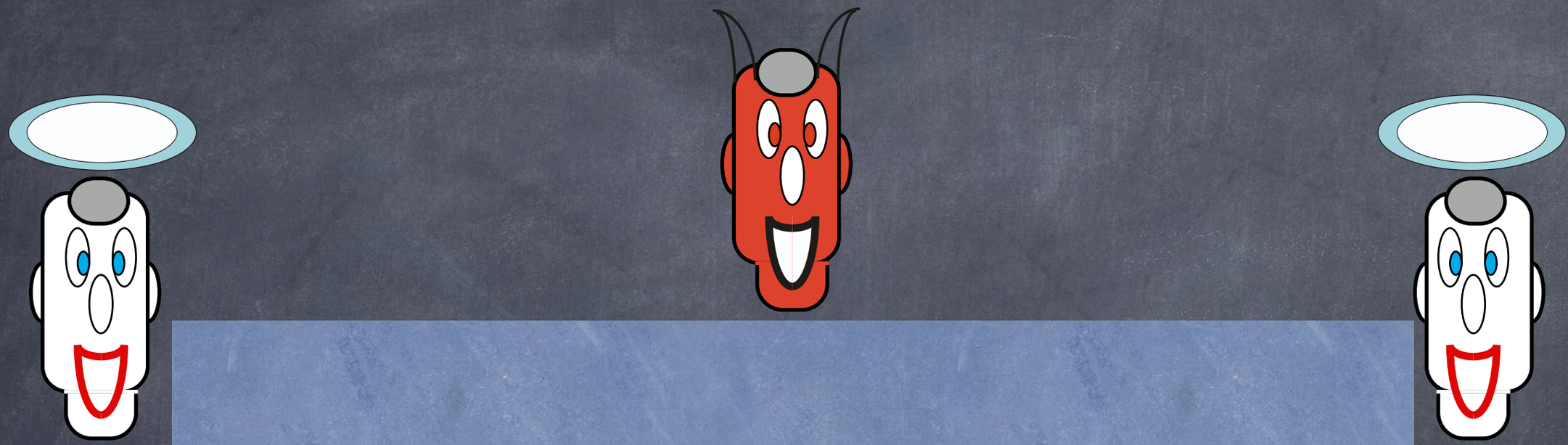
One-Time Identification



Quantum

Cryptography

Information Theoretical Cryptography

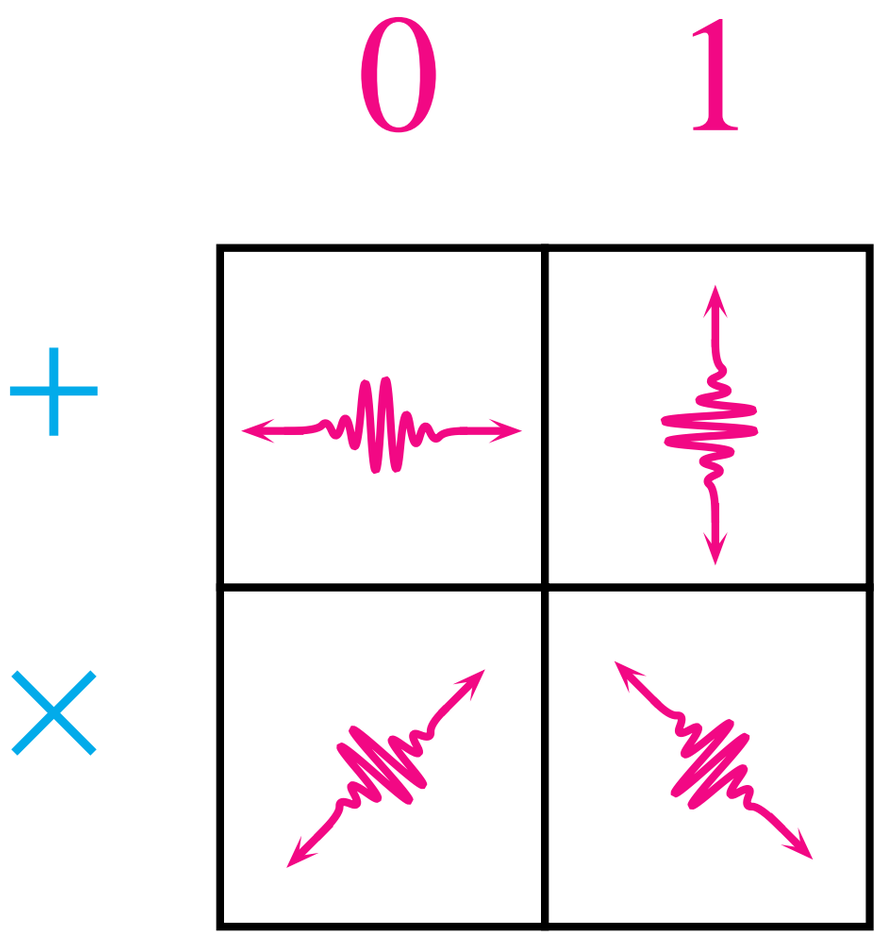


. . . . .

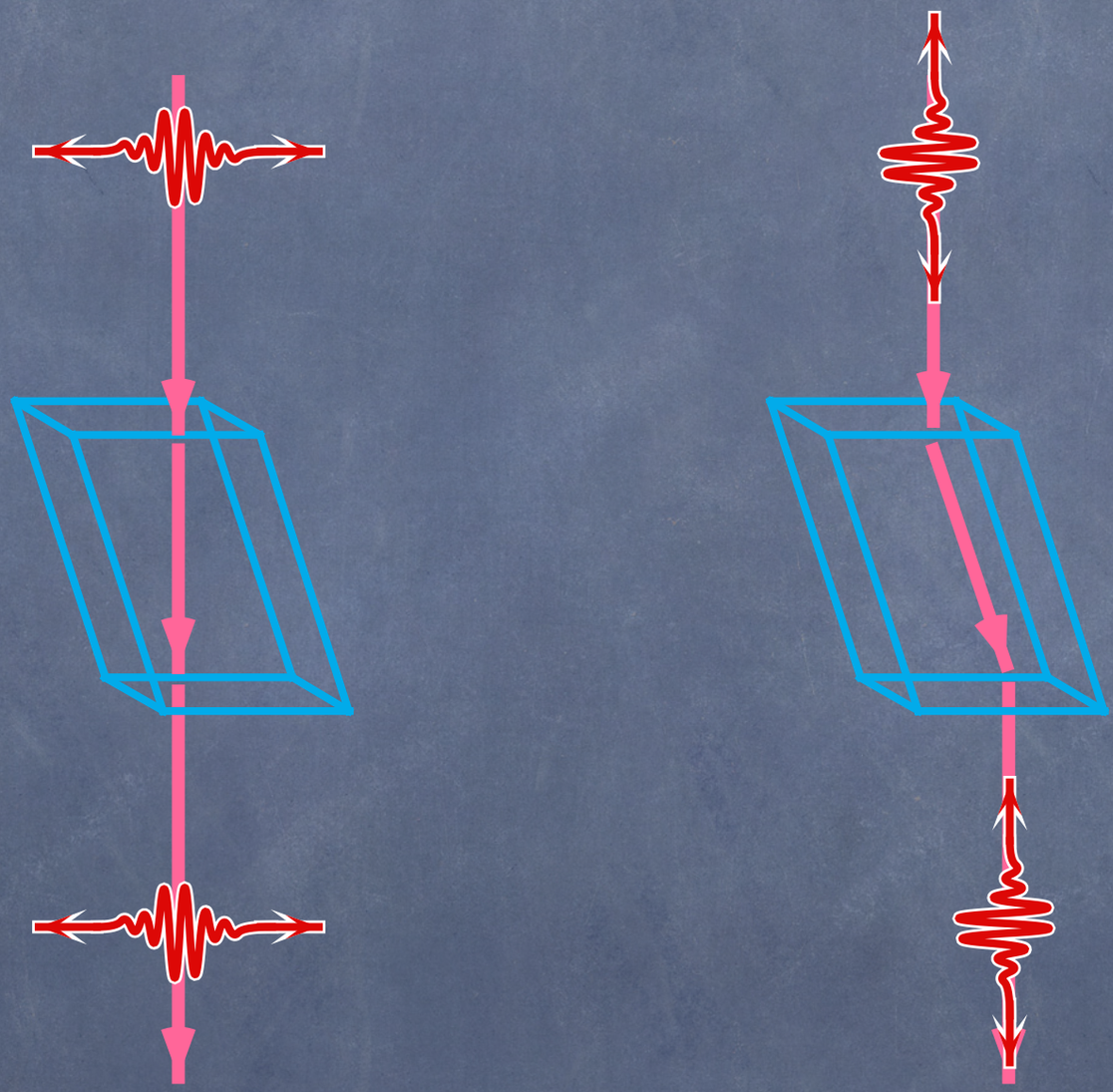
Quantum key distribution

. . . . .

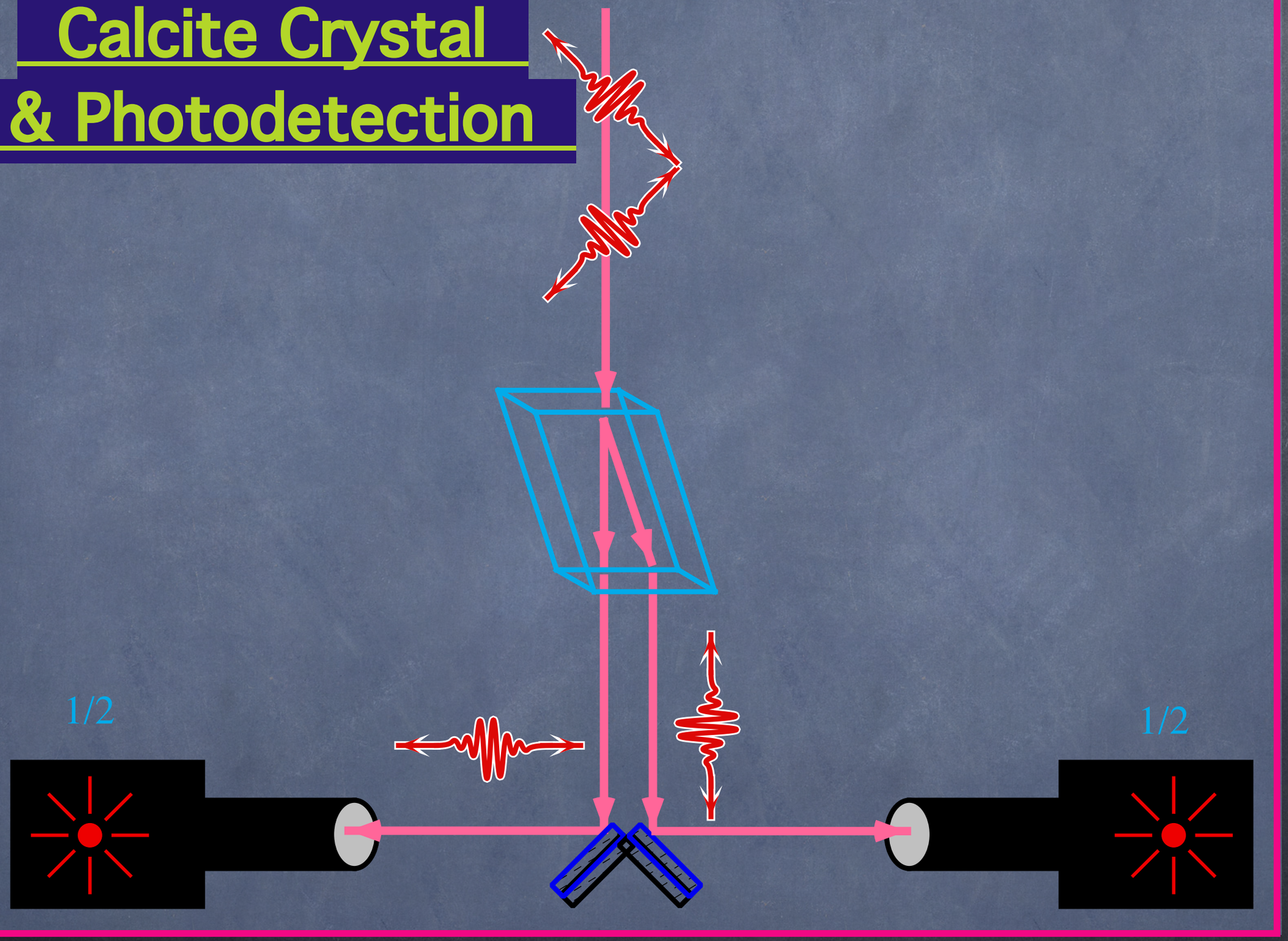
Ambiguous Coding Scheme



Calcite Crystal

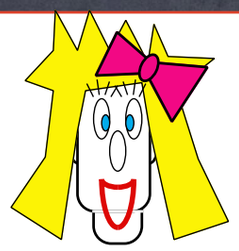


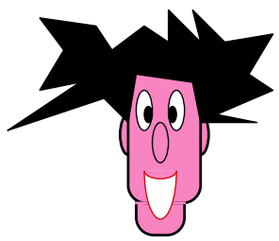
Calcite Crystal & Photodetection



Quantum Key Distribution

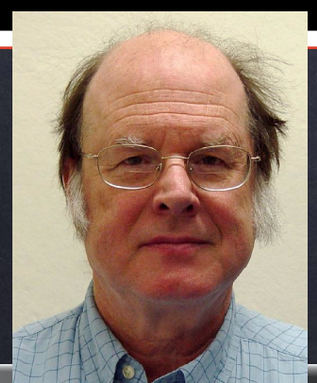
Quantum Key Distribution





A:	0	1	1	0	0	1	0	0	1	1	0	1	0	0	0	1	1	1	0	1	1	0	0	0
	×	+	×	+	+	+	×	×	×	×	+	+	+	+	×	×	×	+	×	+	+	+	×	+
B:	×	×	+	+	×	+	+	+	×	+	+	×	×	×	+	×	×	×	+	+	×	+	×	+
	0	0	1	0	0	1	0	0	1	0	0	0	0	1	1	1	0	0	0	1	1	0	0	0
A:	×	+	×	+	+	+	×	×	×	×	+	+	+	+	×	×	×	+	×	+	+	+	×	+
B:	0	↯	↯	0	↯	1	↯	↯	1	↯	0	↯	↯	↯	↯	1	0	↯	↯	1	↯	0	0	0
B:	0			0		1			1		0					1	0			1		0	0	0
A:	0			0		1			1		0					1	1			1		0	0	0
A:	0					1					0						1							0
B:	=					=					=						≠							=
B:				0				1					1					1		0	0			
A:				0				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 very secret classical key

.....

COMP 102A, Lecture 15

Introduction to Cryptography

COMP 102A, Lecture 15