

Cryptography: the cast

Cryptography: the cast

Alice...

Cryptography: the cast

Alice...



© John Tenniel 1865

Cryptography: the cast

Alice...



© John Tenniel 1865

wishes to send messages to, and receive messages from...

Bob

Bob



© Keith Chapman 1998

Bob



© Keith Chapman 1998

securely. Their opponent is the eavesdropper. . .

Eve

Eve



© Lucas Cranach 1547

Eve



© Lucas Cranach 1547

who is extremely clever and has access to considerable, but not unlimited, computing power. They communicate via a reliable postman. . .

Pat (obviously)



© Ivor Wood 1981

Pat (obviously)



© Ivor Wood 1981

who will deliver correctly any message he is sent but is unable to prevent Eve from reading it on the way. For real-world applications it is also necessary to be wary of...

Fred



© Hanna-Barbera 1960

Fred



© Hanna-Barbera 1960

a fool, who will instantly publish any data that comes his way.

We are going to consider the problem mainly from the point of view of Alice.

We are going to consider the problem mainly from the point of view of Alice.

She cannot trust anybody except Pat

We are going to consider the problem mainly from the point of view of Alice.

She cannot trust anybody except Pat (we shall deal later with the problems that arise if Pat is unreliable)

We are going to consider the problem mainly from the point of view of Alice.

She cannot trust anybody except Pat (we shall deal later with the problems that arise if Pat is unreliable) and he is limited to a single function.

We are going to consider the problem mainly from the point of view of Alice.

She cannot trust anybody except Pat (we shall deal later with the problems that arise if Pat is unreliable) and he is limited to a single function. Eve is hostile;

We are going to consider the problem mainly from the point of view of Alice.

She cannot trust anybody except Pat (we shall deal later with the problems that arise if Pat is unreliable) and he is limited to a single function. Eve is hostile; Bob is not trustworthy.

We are going to consider the problem mainly from the point of view of Alice.

She cannot trust anybody except Pat (we shall deal later with the problems that arise if Pat is unreliable) and he is limited to a single function. Eve is hostile; Bob is not trustworthy. Fred is beyond the reach even of mathematics.

We are going to consider the problem mainly from the point of view of Alice.

She cannot trust anybody except Pat (we shall deal later with the problems that arise if Pat is unreliable) and he is limited to a single function. Eve is hostile; Bob is not trustworthy. Fred is beyond the reach even of mathematics.

Mit der Dummheit kämpfen Götter selbst vergebens.

© Friedrich Schiller 1801

We are going to consider the problem mainly from the point of view of Alice.

She cannot trust anybody except Pat (we shall deal later with the problems that arise if Pat is unreliable) and he is limited to a single function. Eve is hostile; Bob is not trustworthy. Fred is beyond the reach even of mathematics.

Mit der Dummheit kämpfen Götter selbst vergebens.

© Friedrich Schiller 1801

It is impossible to make anything foolproof, because fools are so ingenious.

I have failed to trace the © for this one.