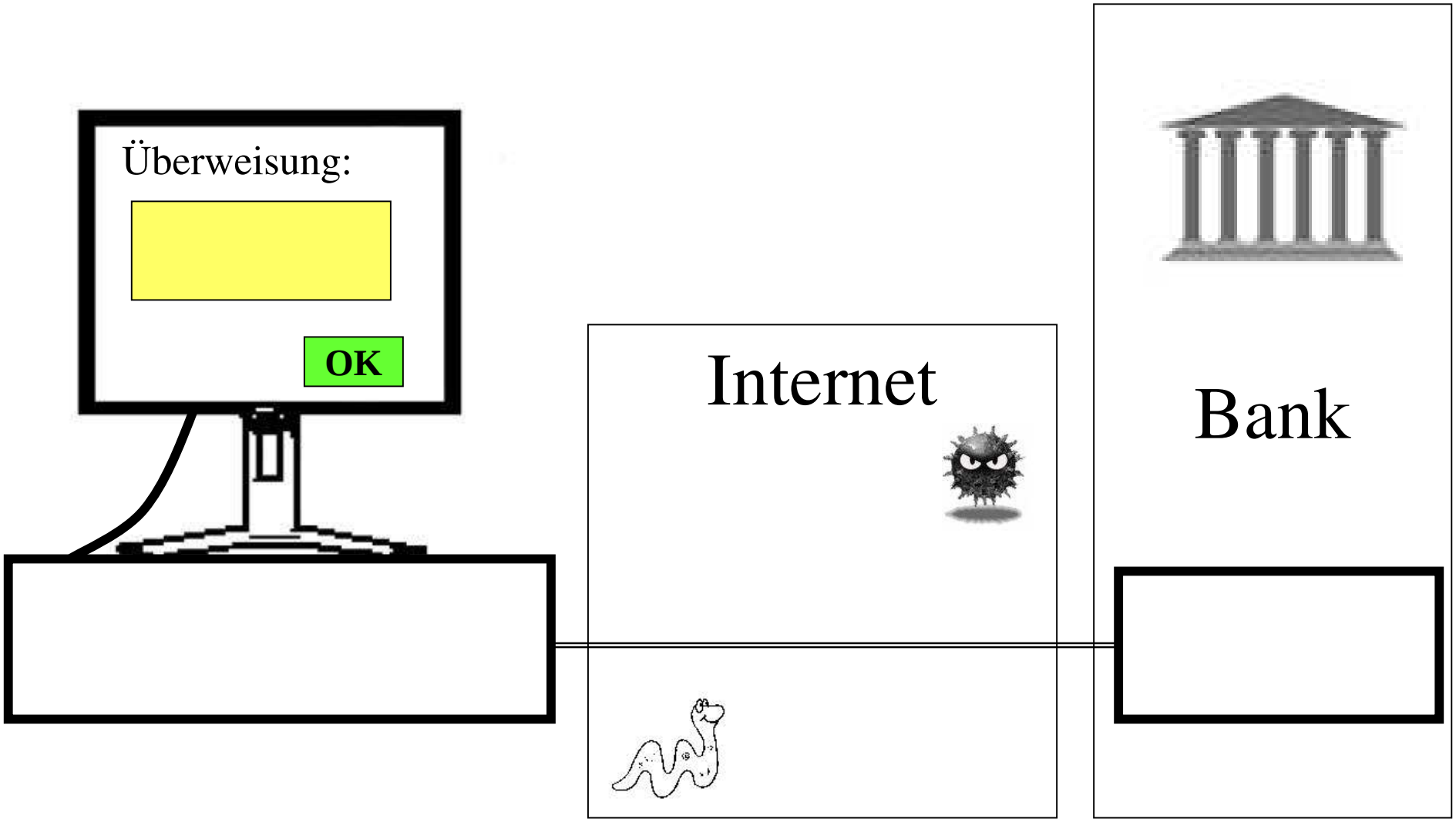
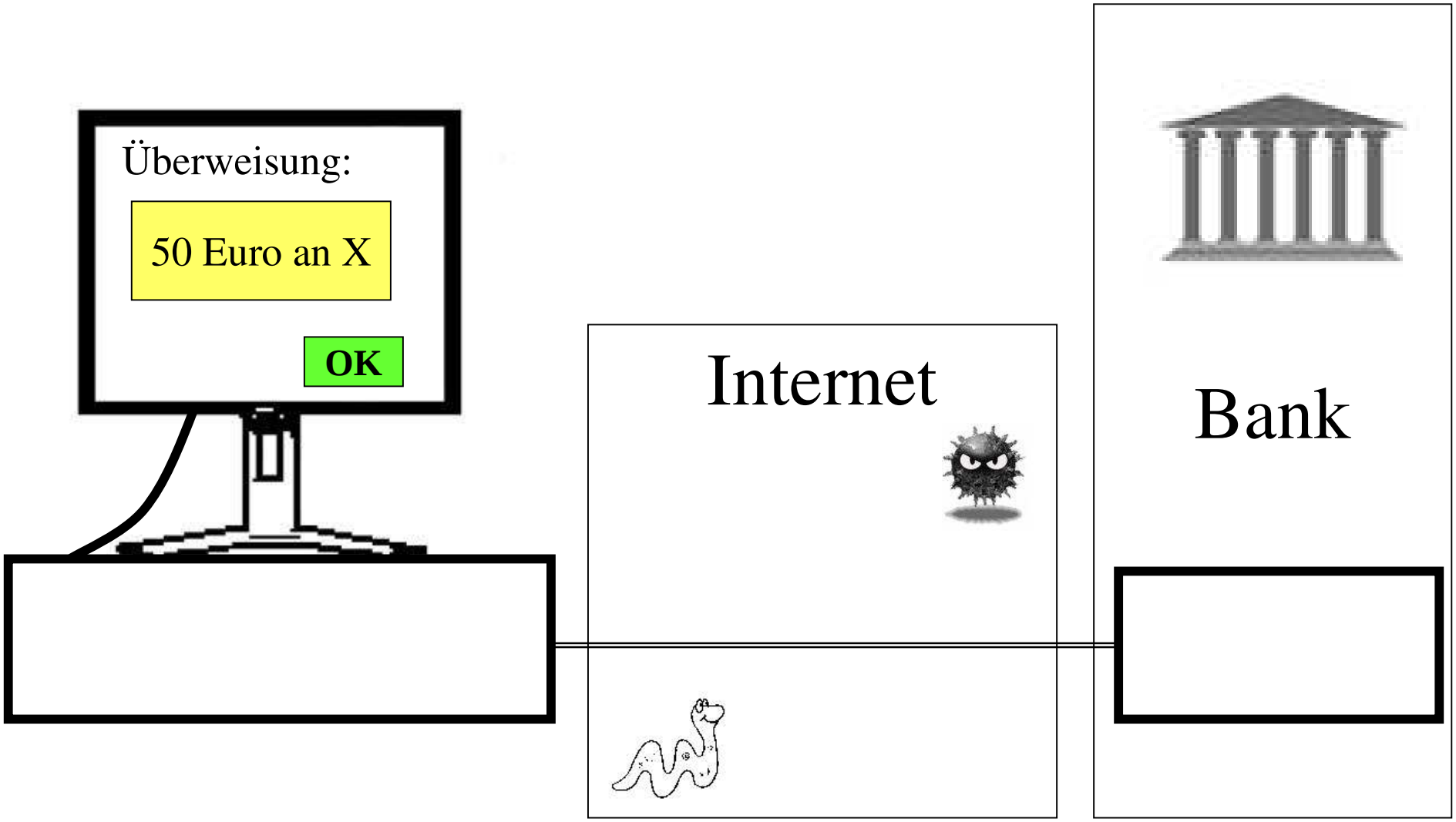
Der Man-in-the-Middle Fälschungs-Angriff auf das iTAN Verfahren

Bernd Borchert, November 2008

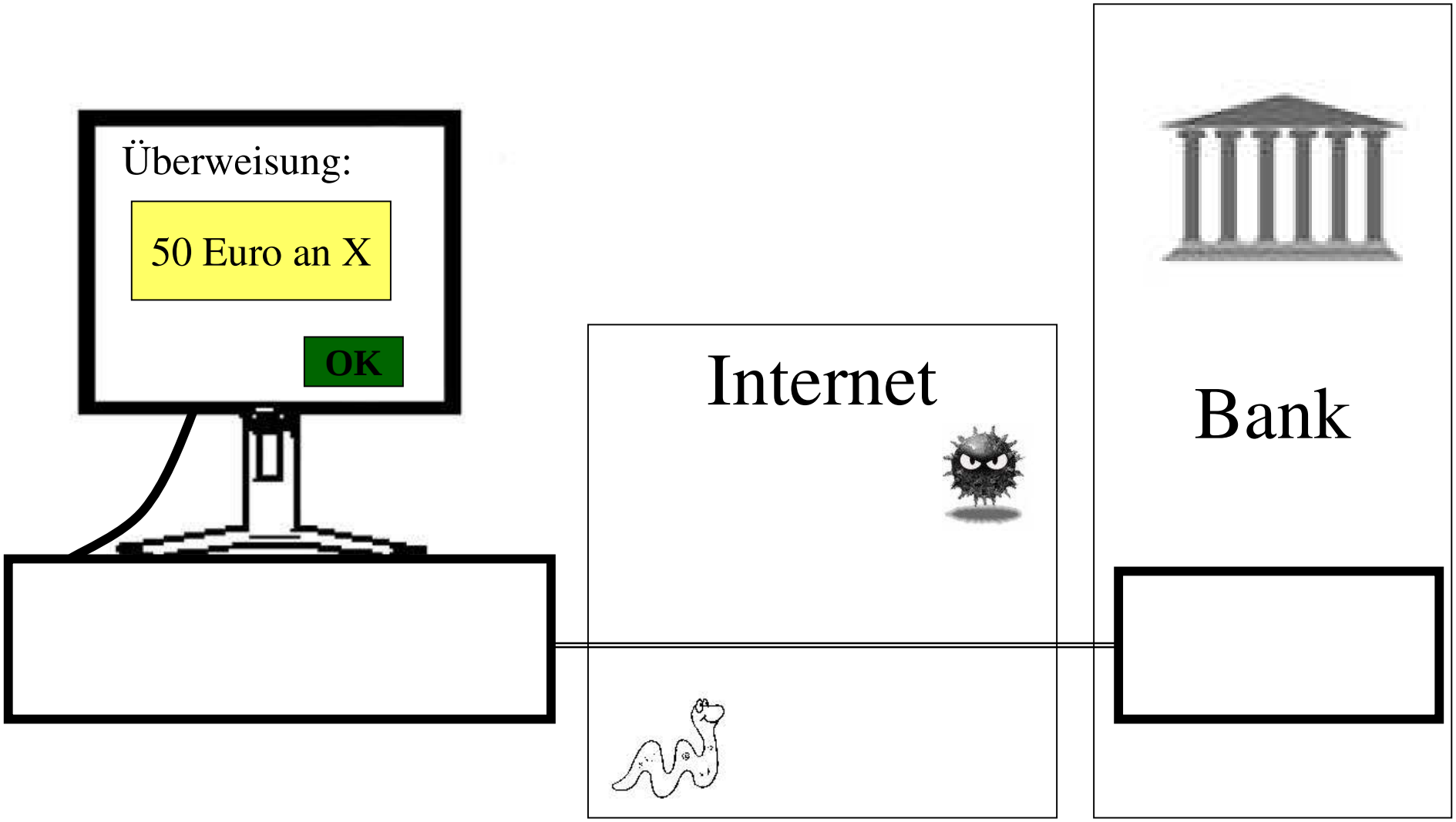
Zuerst wird das reguläre iTAN Verfahren beschrieben - ohne Trojaner.



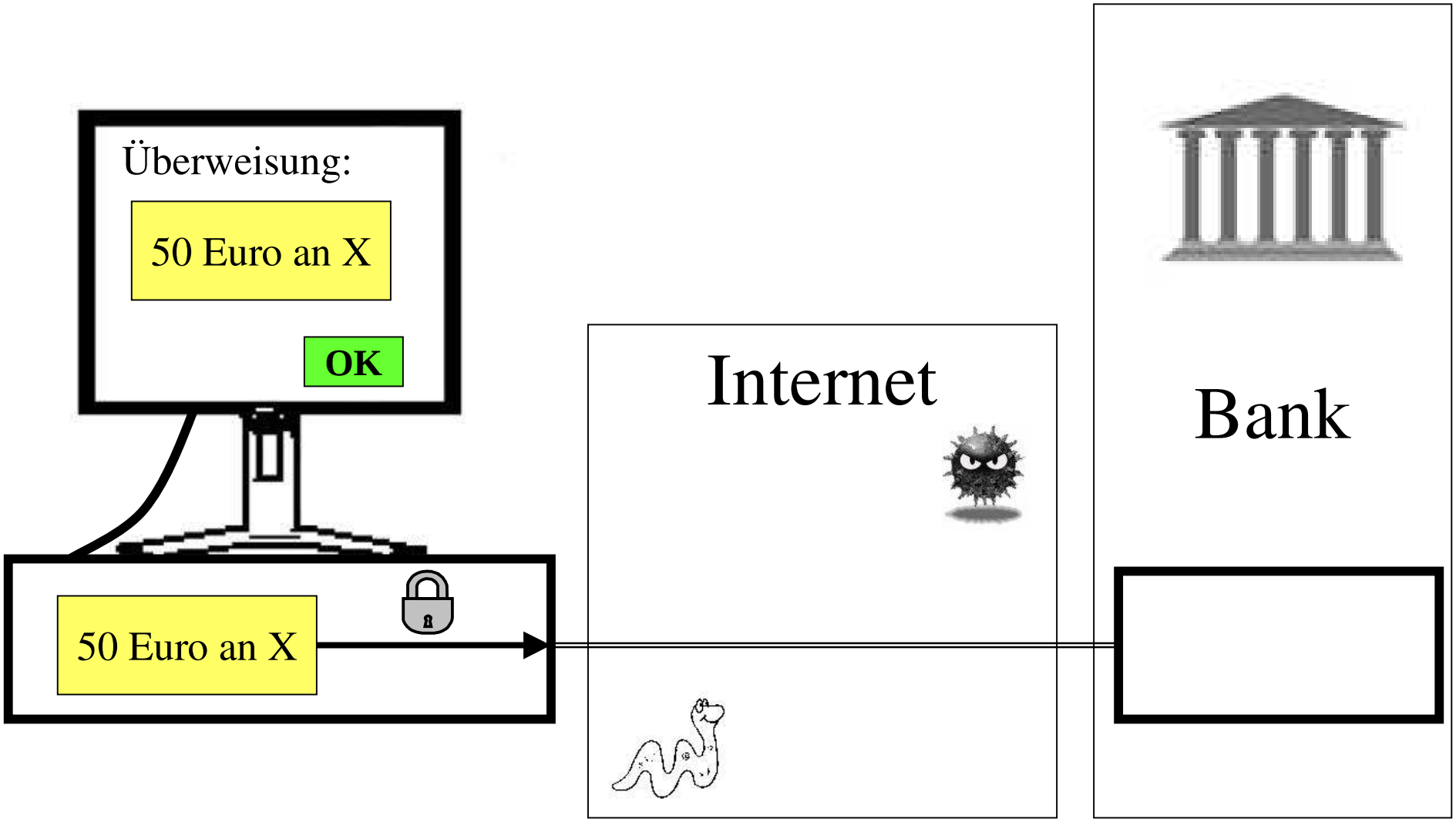
Für die Überweisung wird ein Formular auf dem Bildschirm des Bankkunden angezeigt.



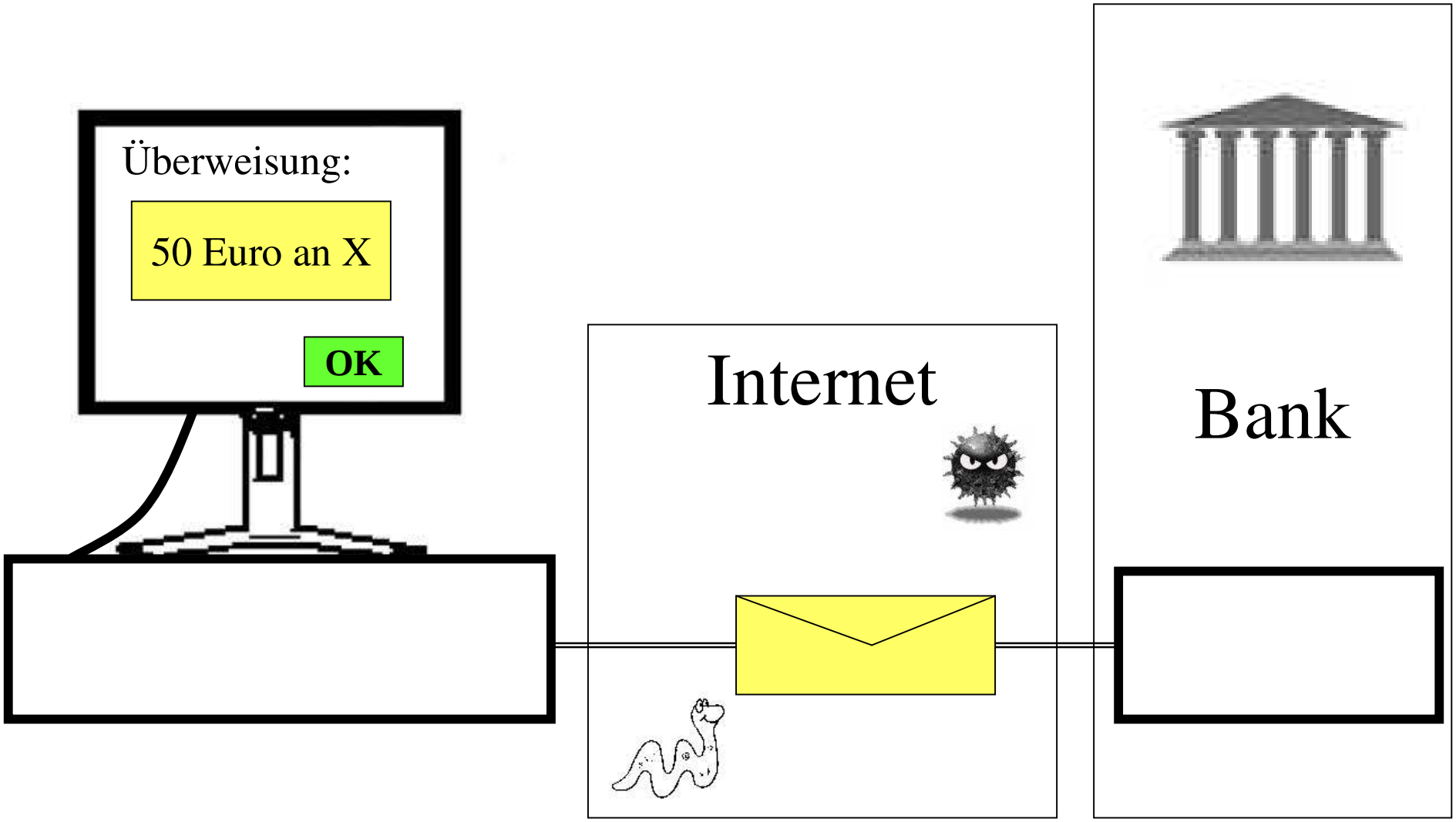
Der Bankkunde füllt das Formular aus.



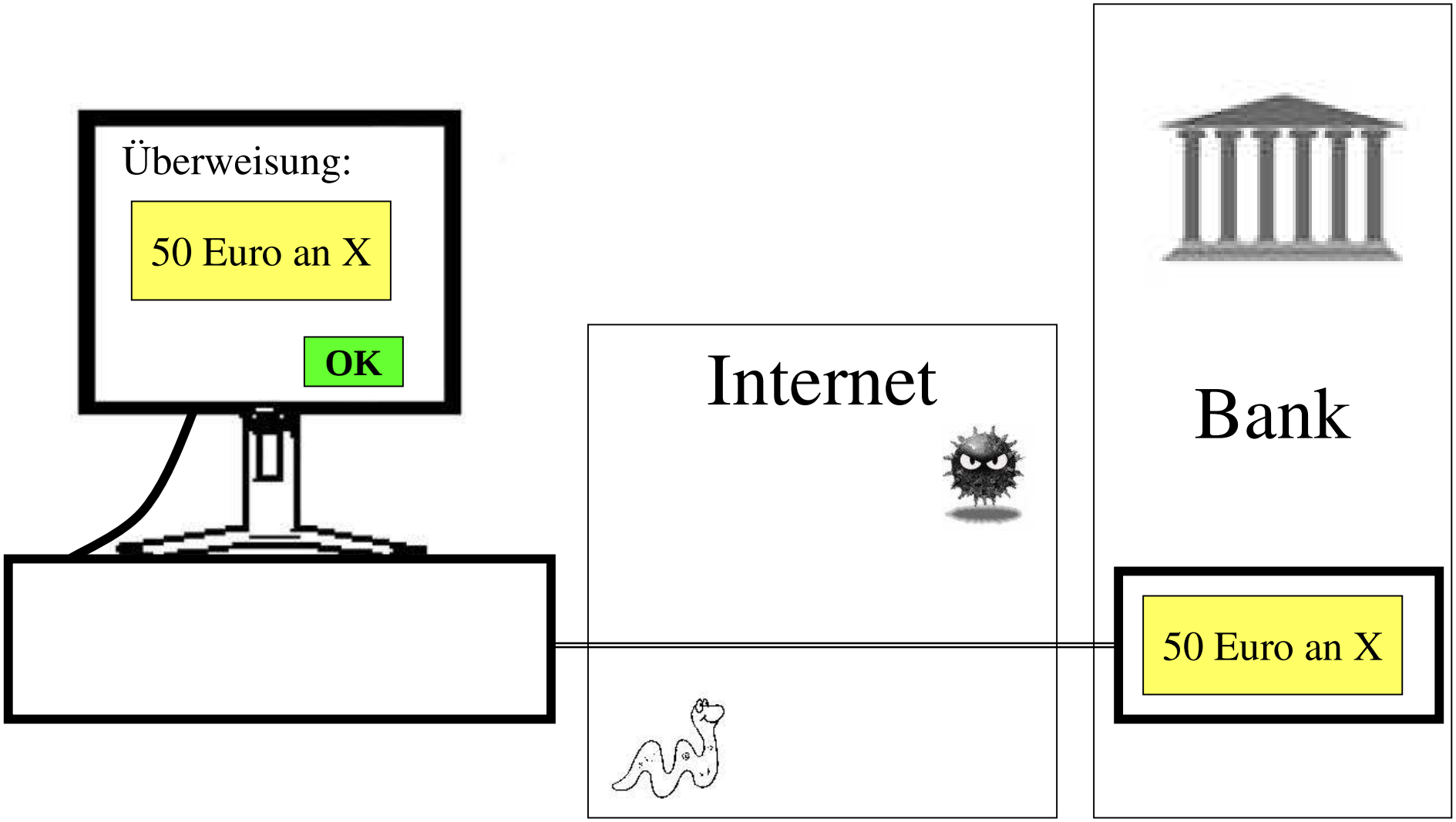
Der Überweisungsauftrag wird „abgeschickt“.



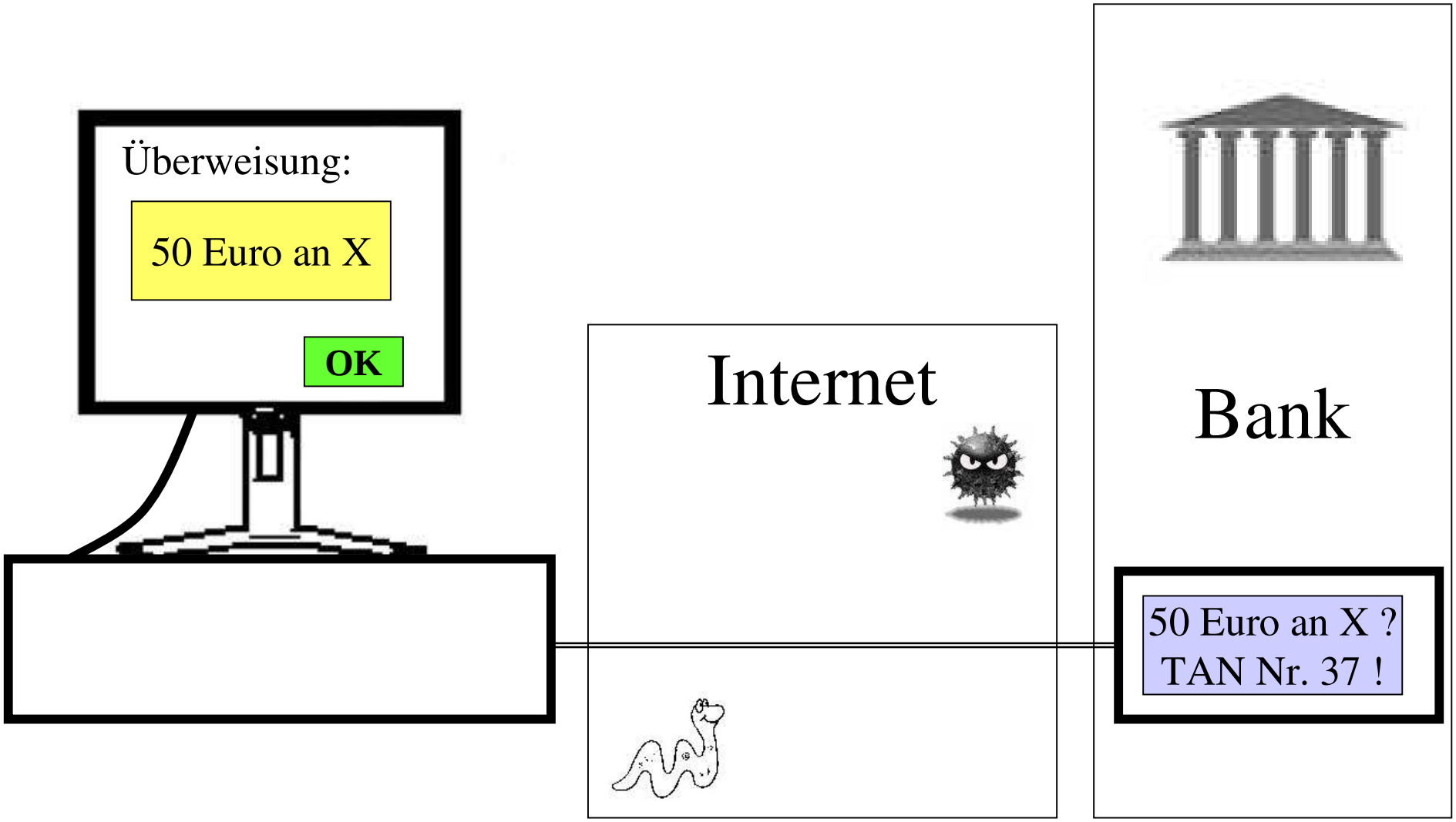
Der Überweisungsauftrag wird verschlüsselt ...



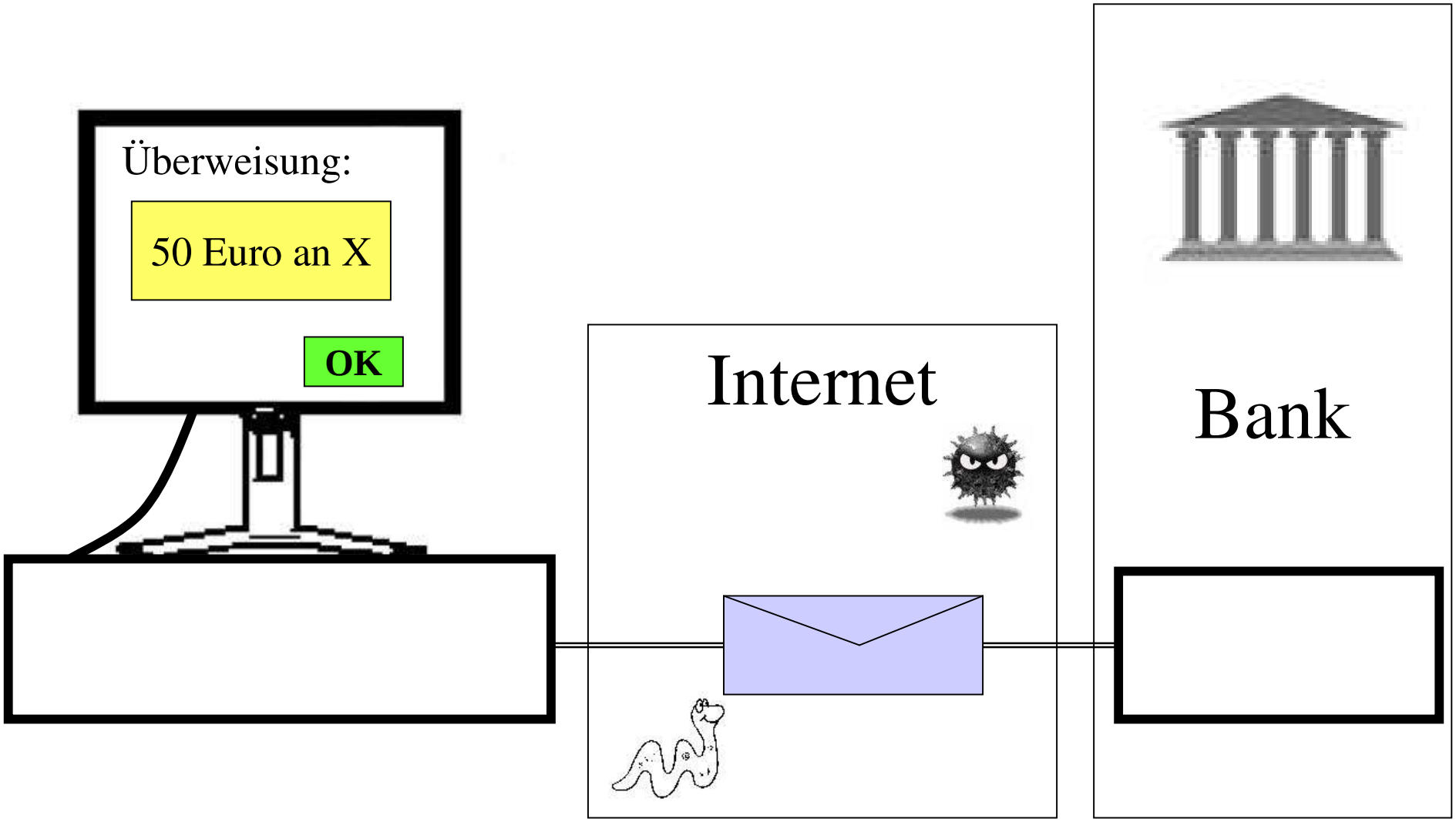
... und durch das Internet an den Bank-Server geschickt.



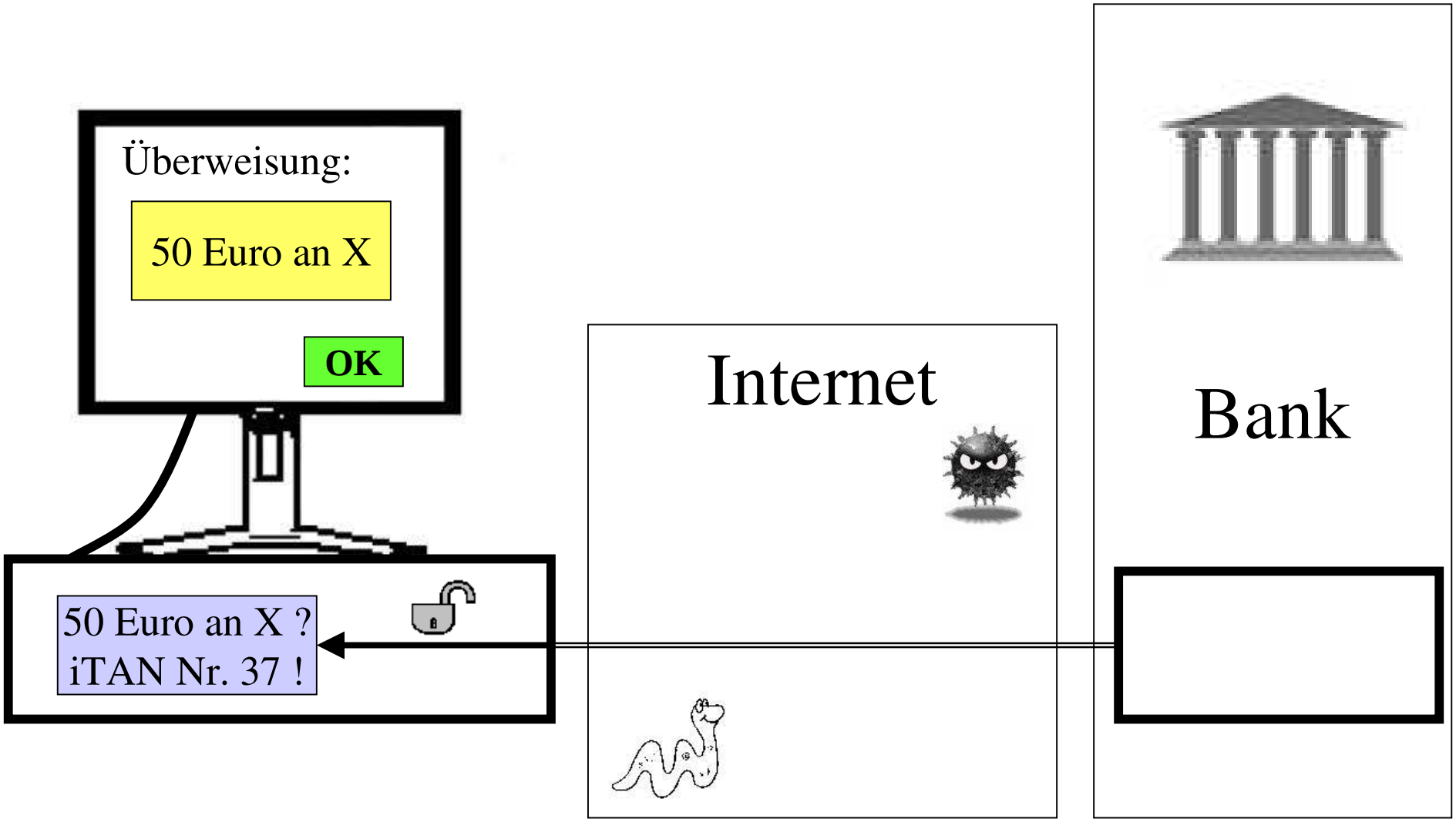
Der Bank-Server entschlüsselt die Nachricht.



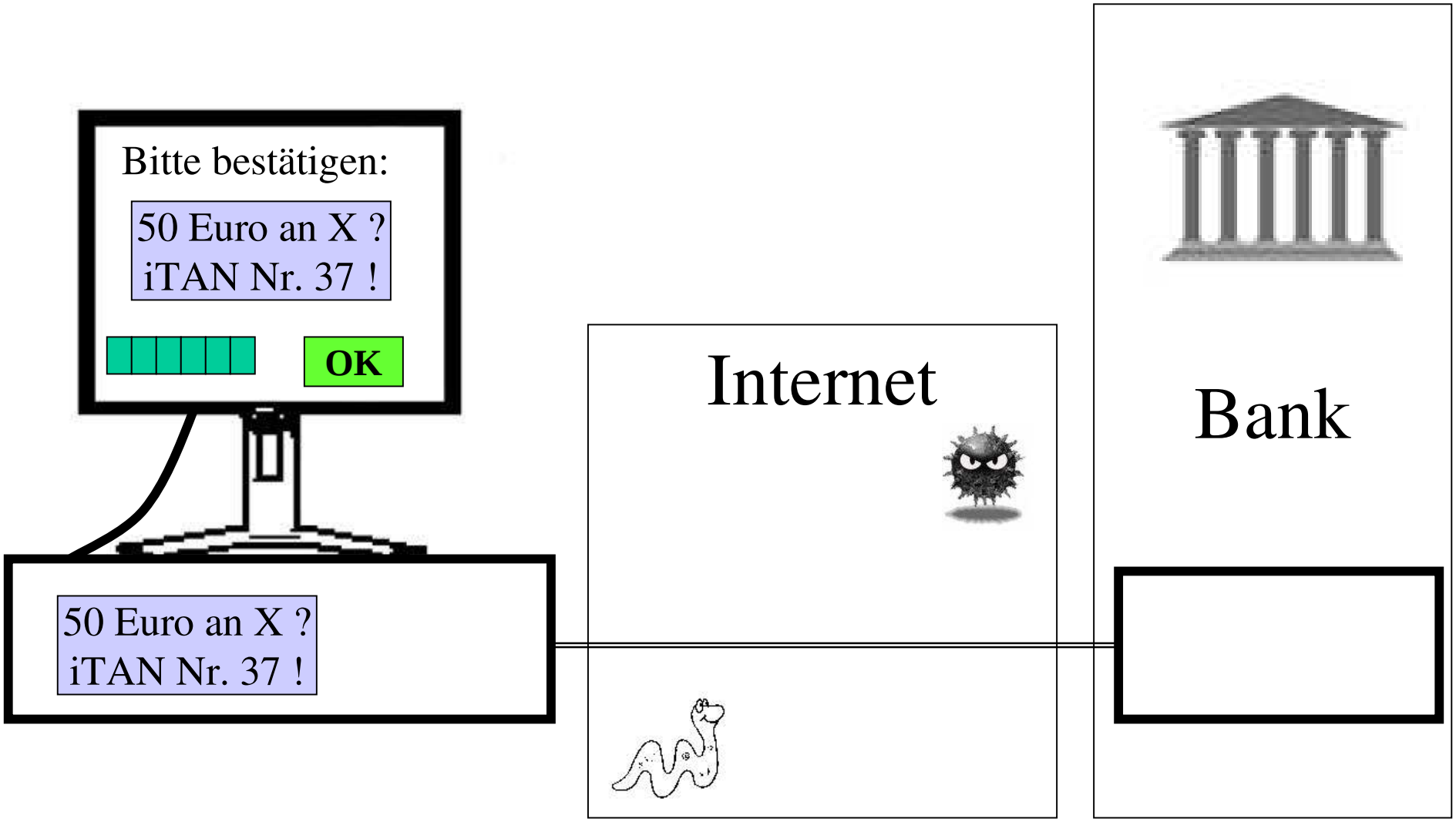
Es wird die iTAN Bestätigungs-Anfrage vorbereitet ...



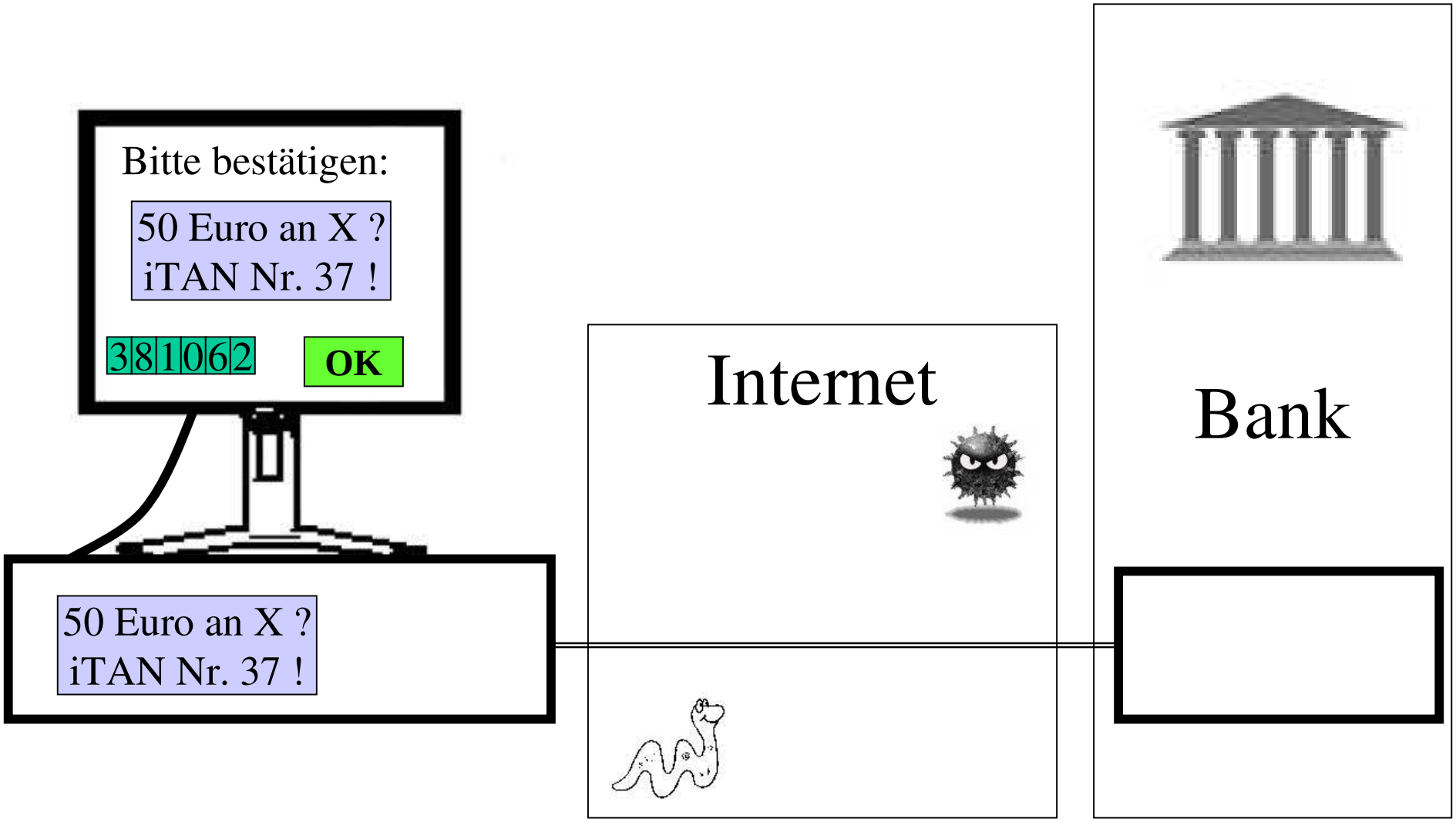
... und verschlüsselt durch das Internet zum Rechner des Bankkunden geschickt.



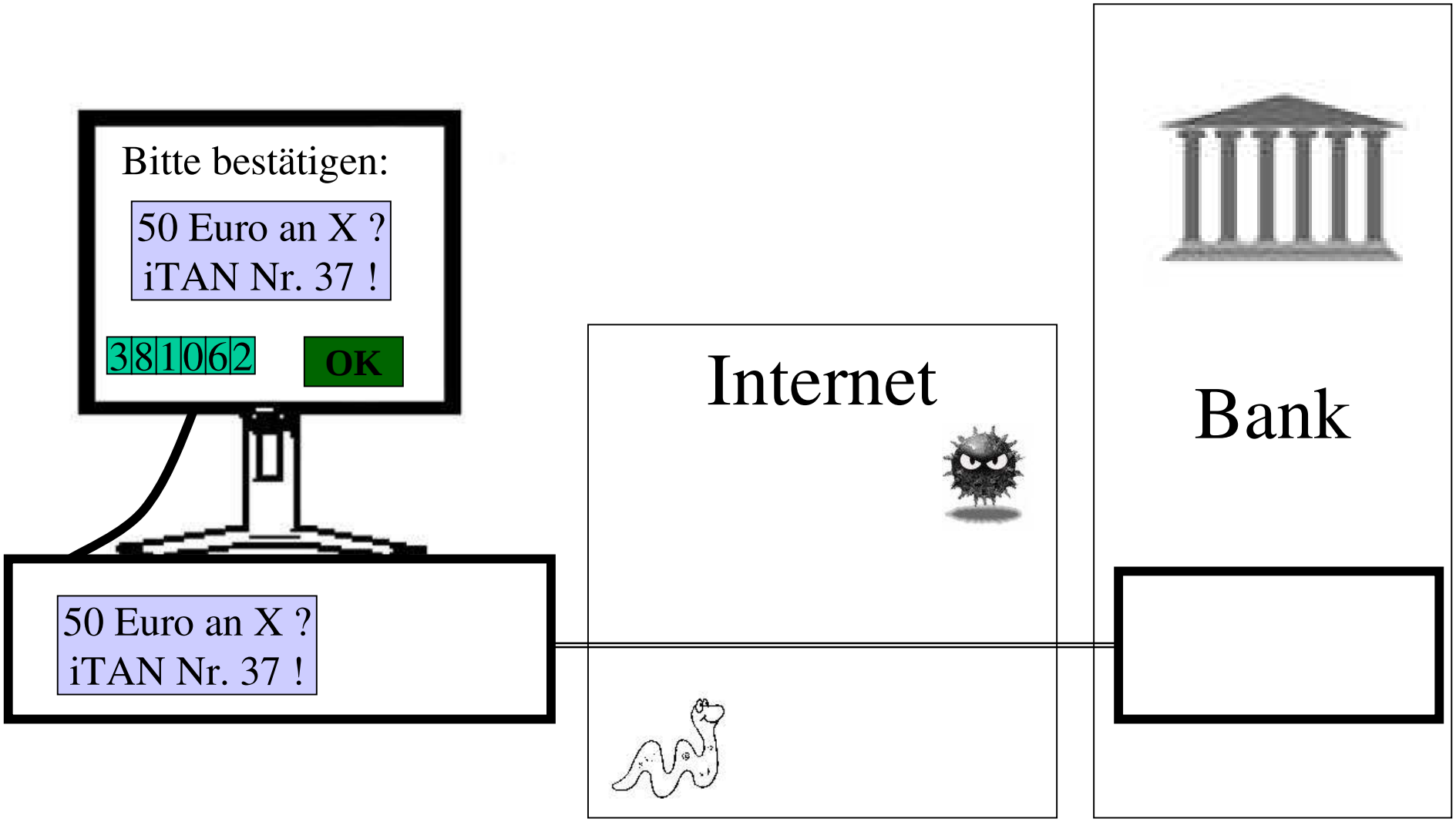
Der Rechner des Bankkunden entschlüsselt die iTAN Bestätigungs-Anfrage.



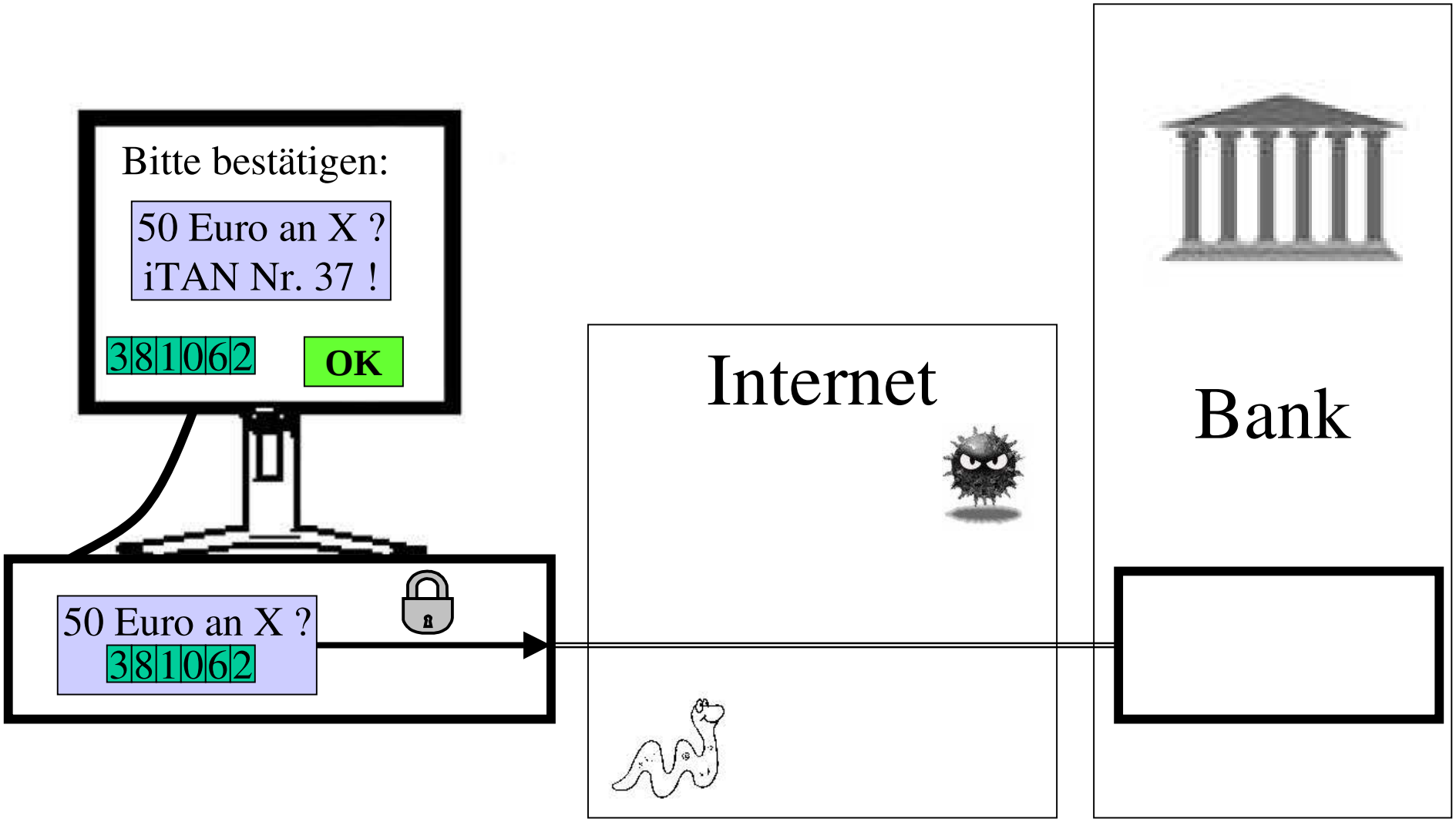
Die iTAN Bestätigungs-Anfrage wird auf dem Bildschirm dargestellt.



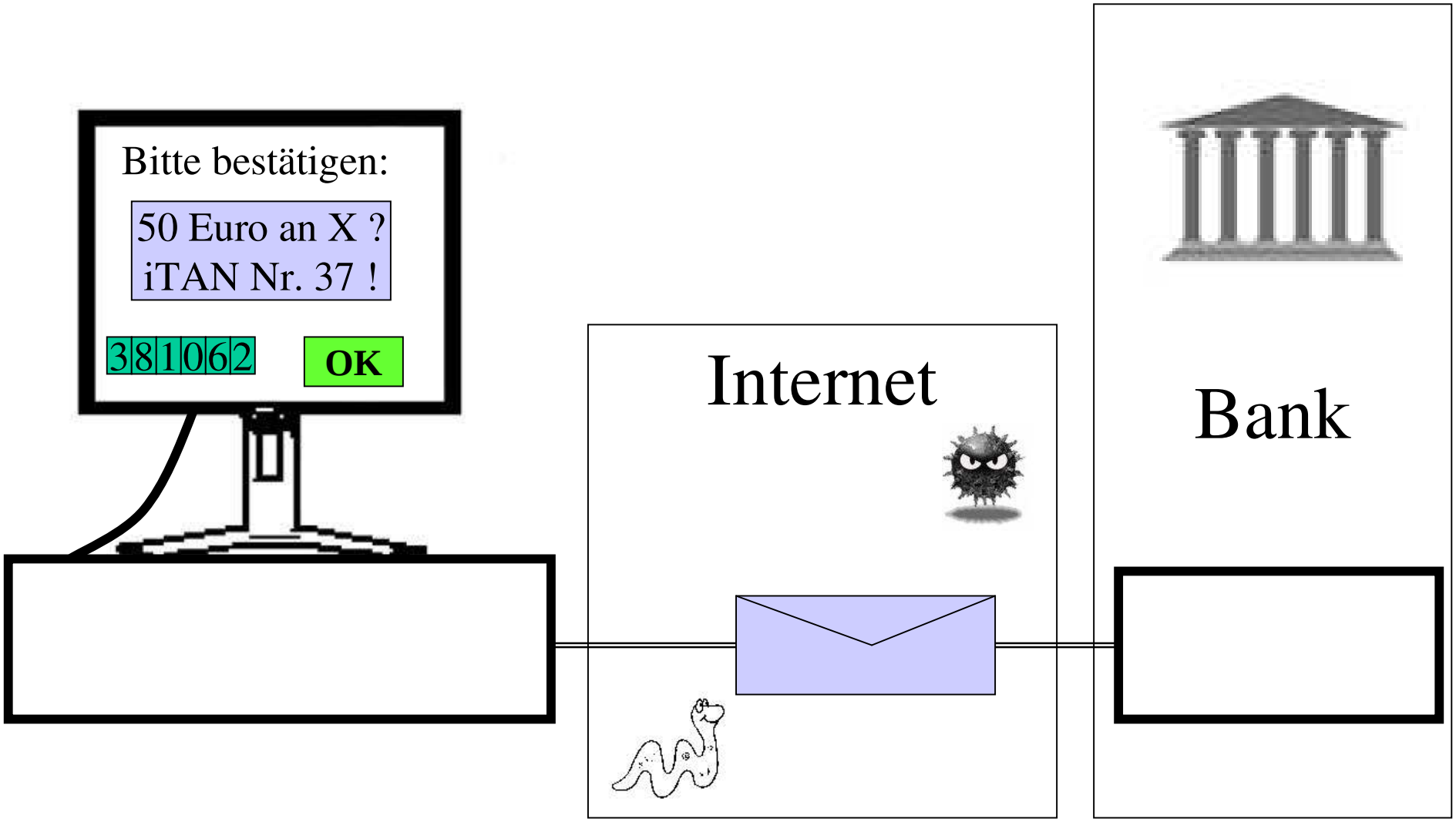
Der Bankkunde gibt die entsprechende iTAN ein.



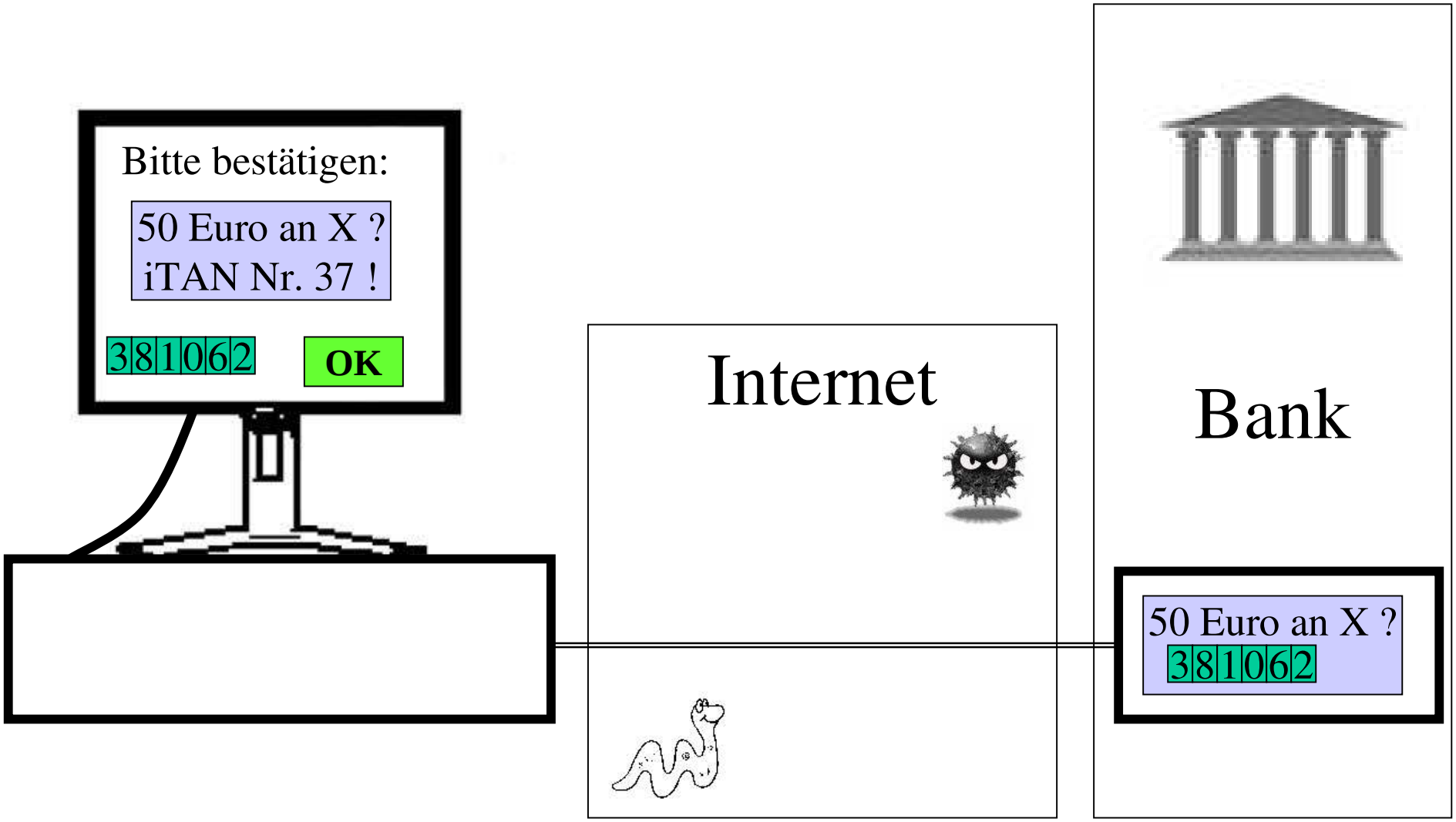
Die iTAN wird vom Bankkunden „abgeschickt“.



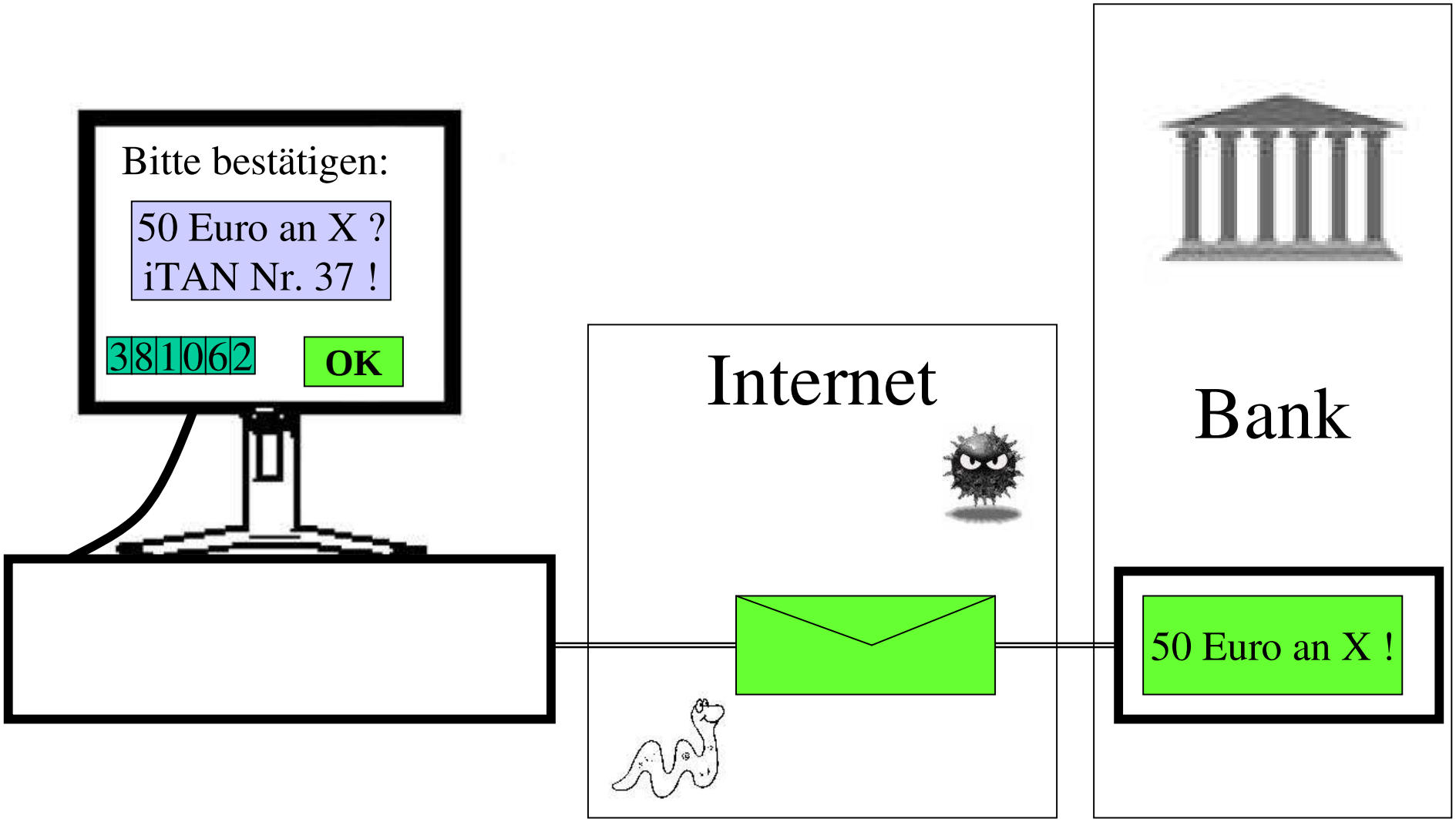
Die iTAN wird verschlüsselt ...



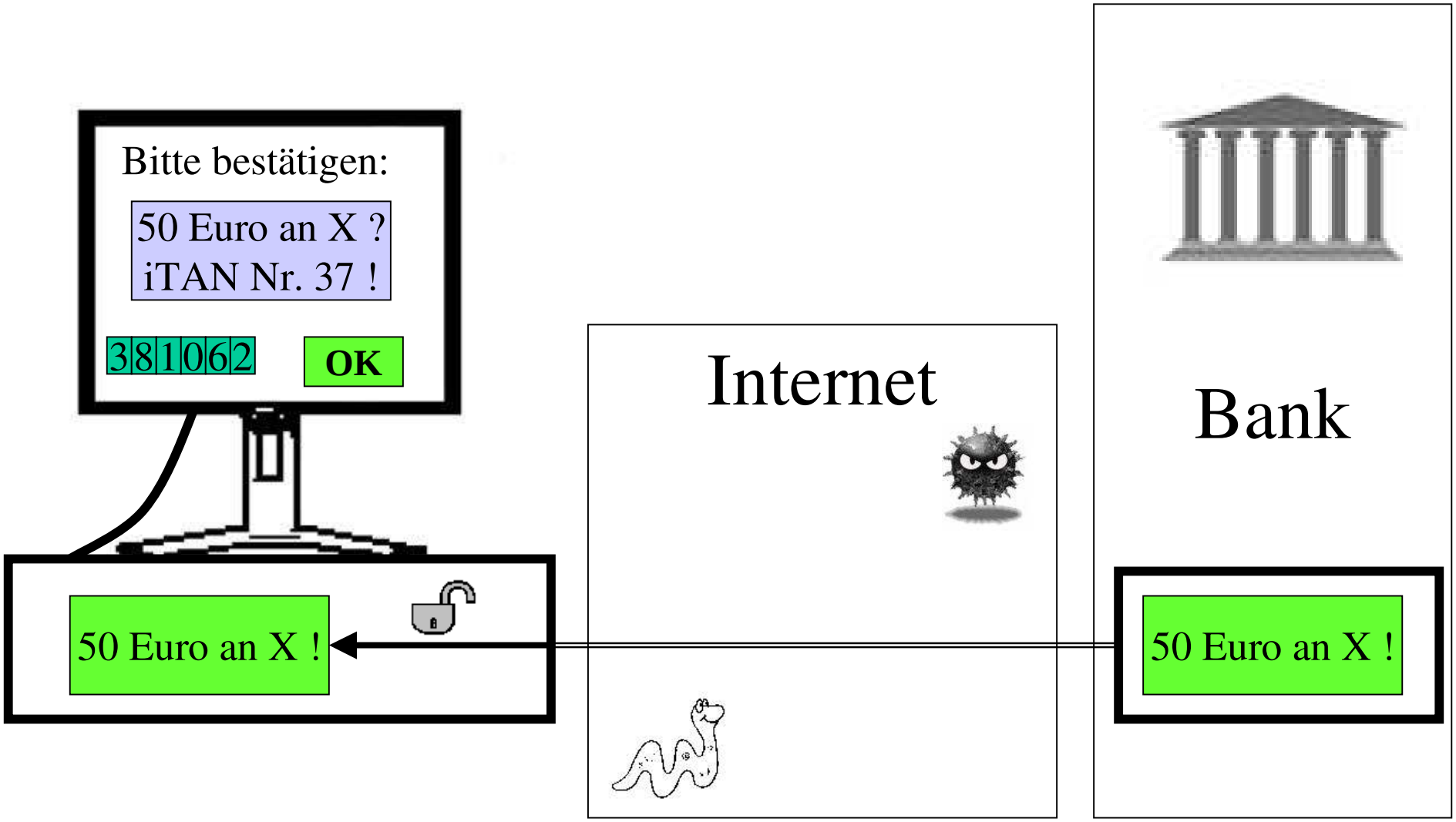
... und durch das Internet zum Bank-Server geschickt.



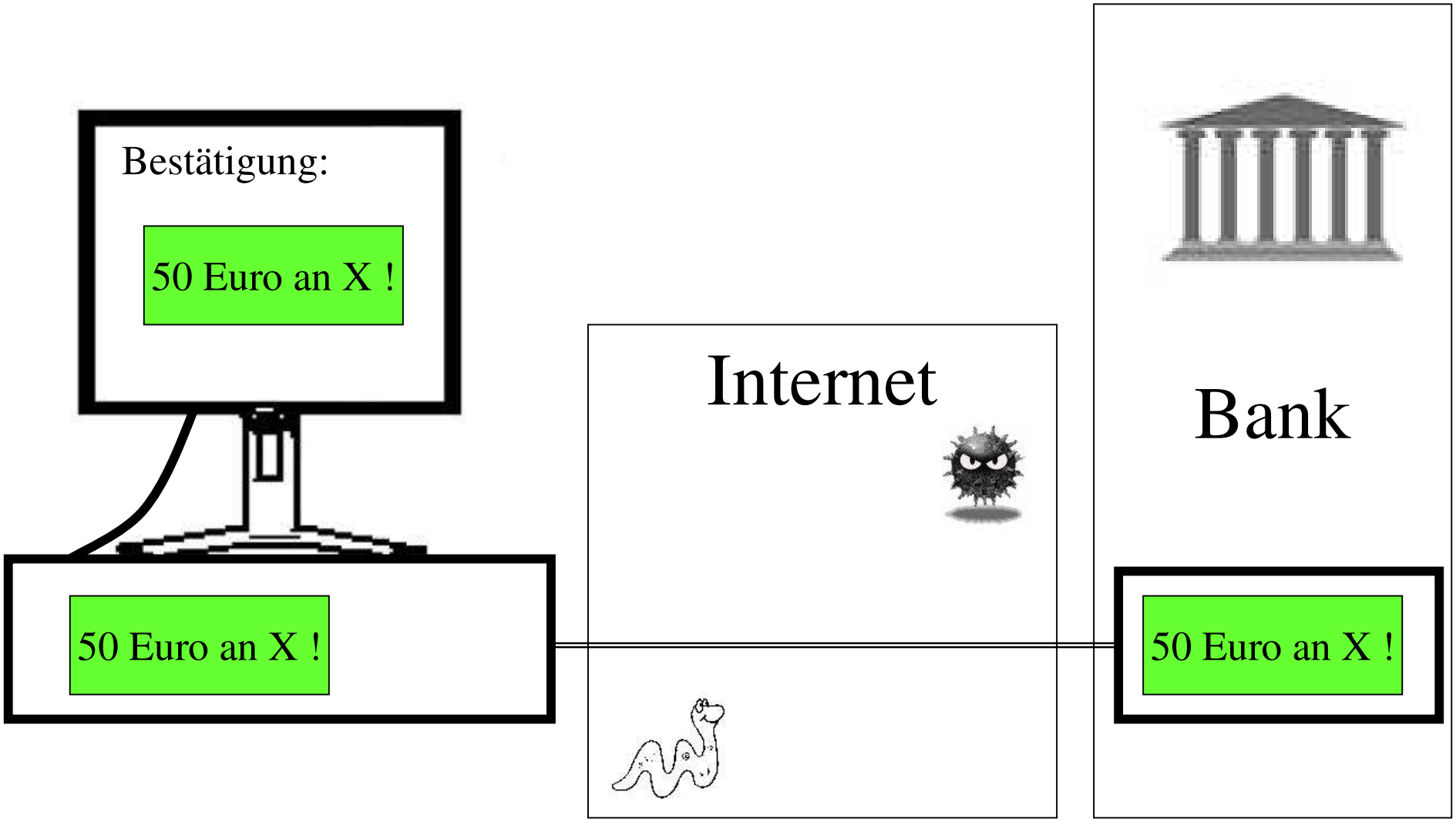
Der Bank-Server entschlüsselt die Nachricht überprüft die Richtigkeit der iTAN.



Wenn die iTAN richtig war, wird eine Bestätigung zum Bankkunden geschickt.



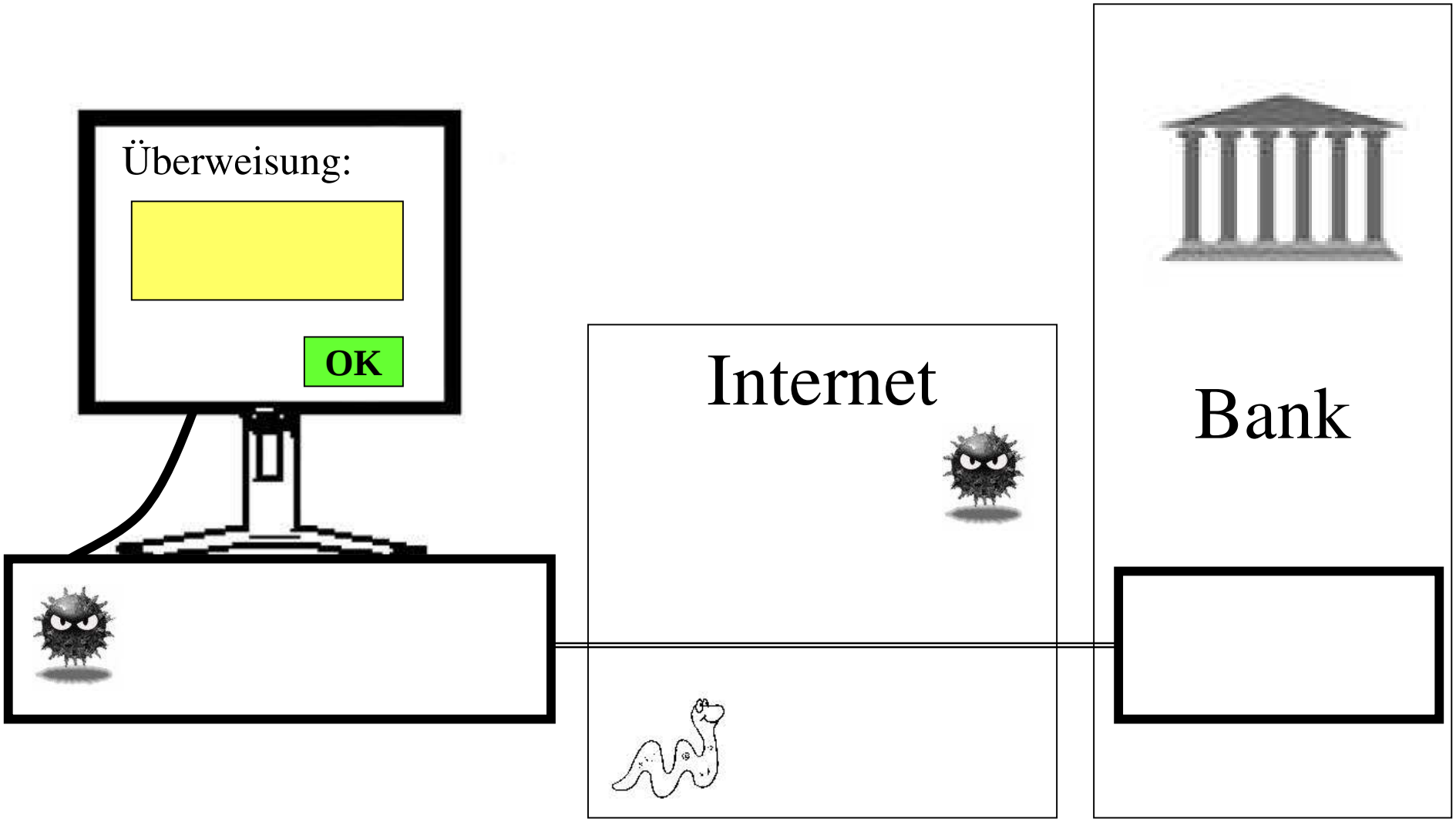
Die Bestätigung wird entschlüsselt ...



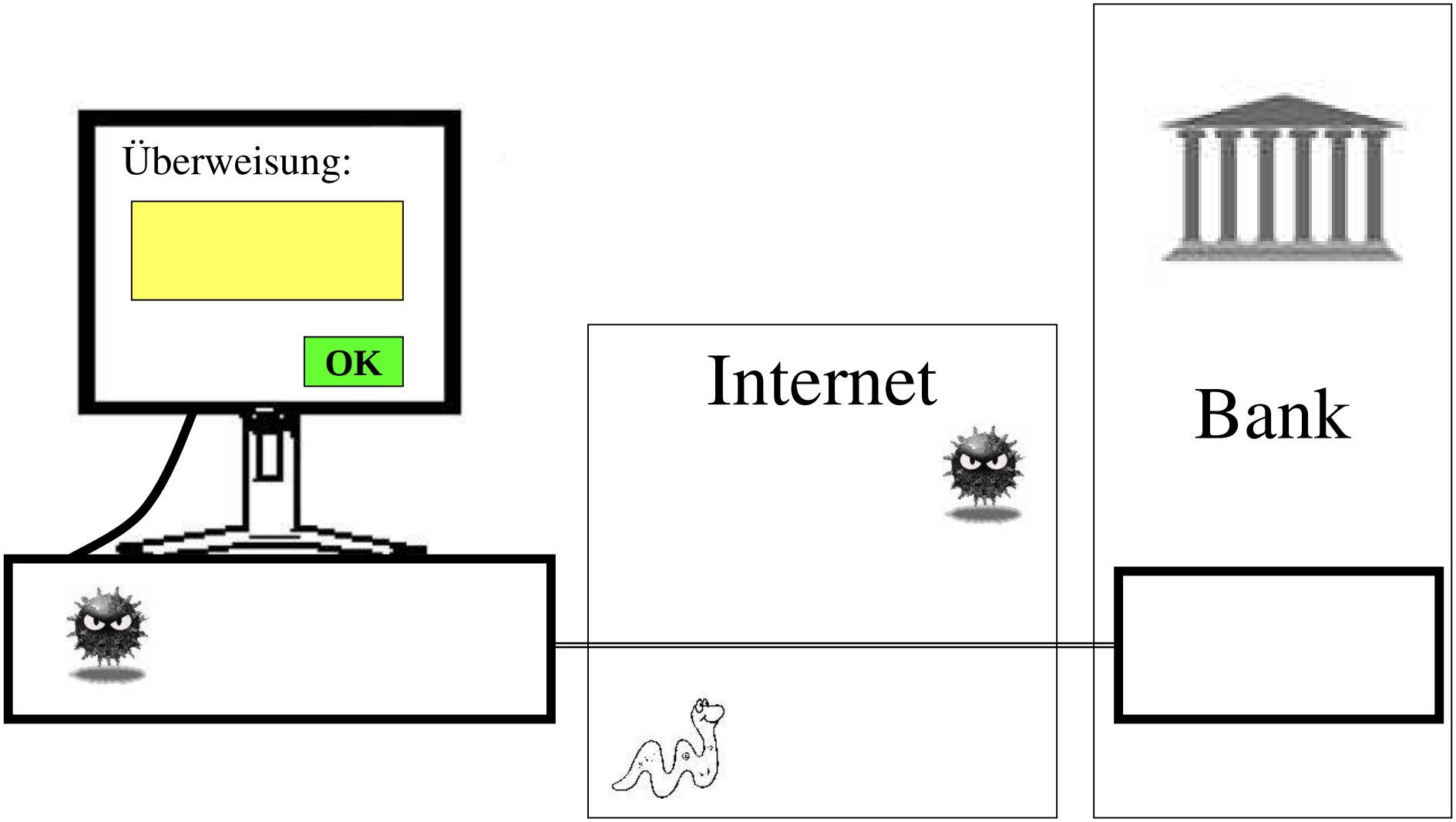
... und auf dem Bildschirm des Bankkunden dargestellt.

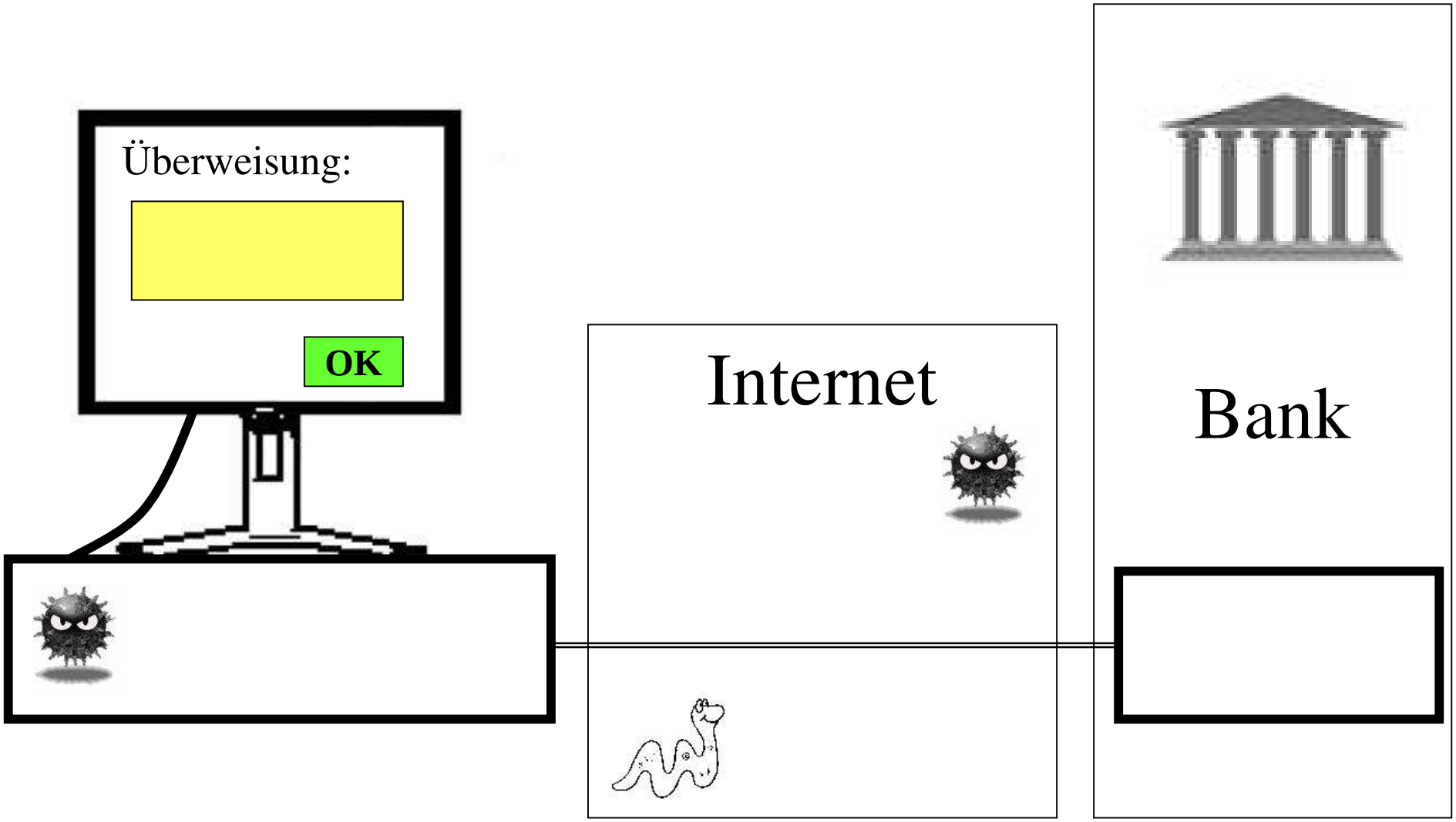
Die Überweisung wurde in der Zwischenzeit von der Bank ausgeführt. Alles ok. Das war‘s.

Und jetzt kommt der Fall, dass sich ein Trojaner auf den Rechner des Bankkunden eingeschlichen hat:

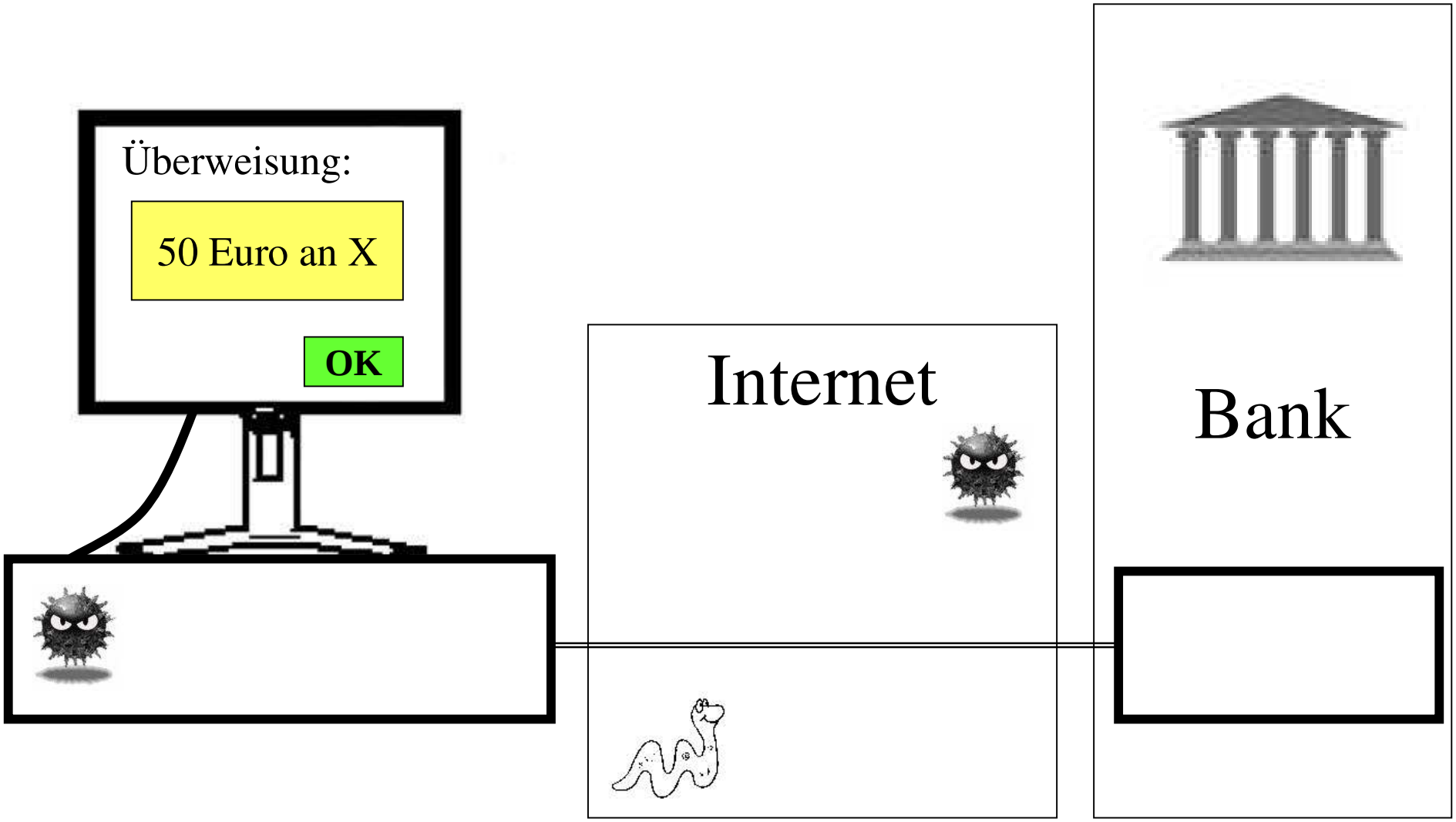


Es befindet sich ein Trojaner-Virus auf dem Rechner des Bankkunden.

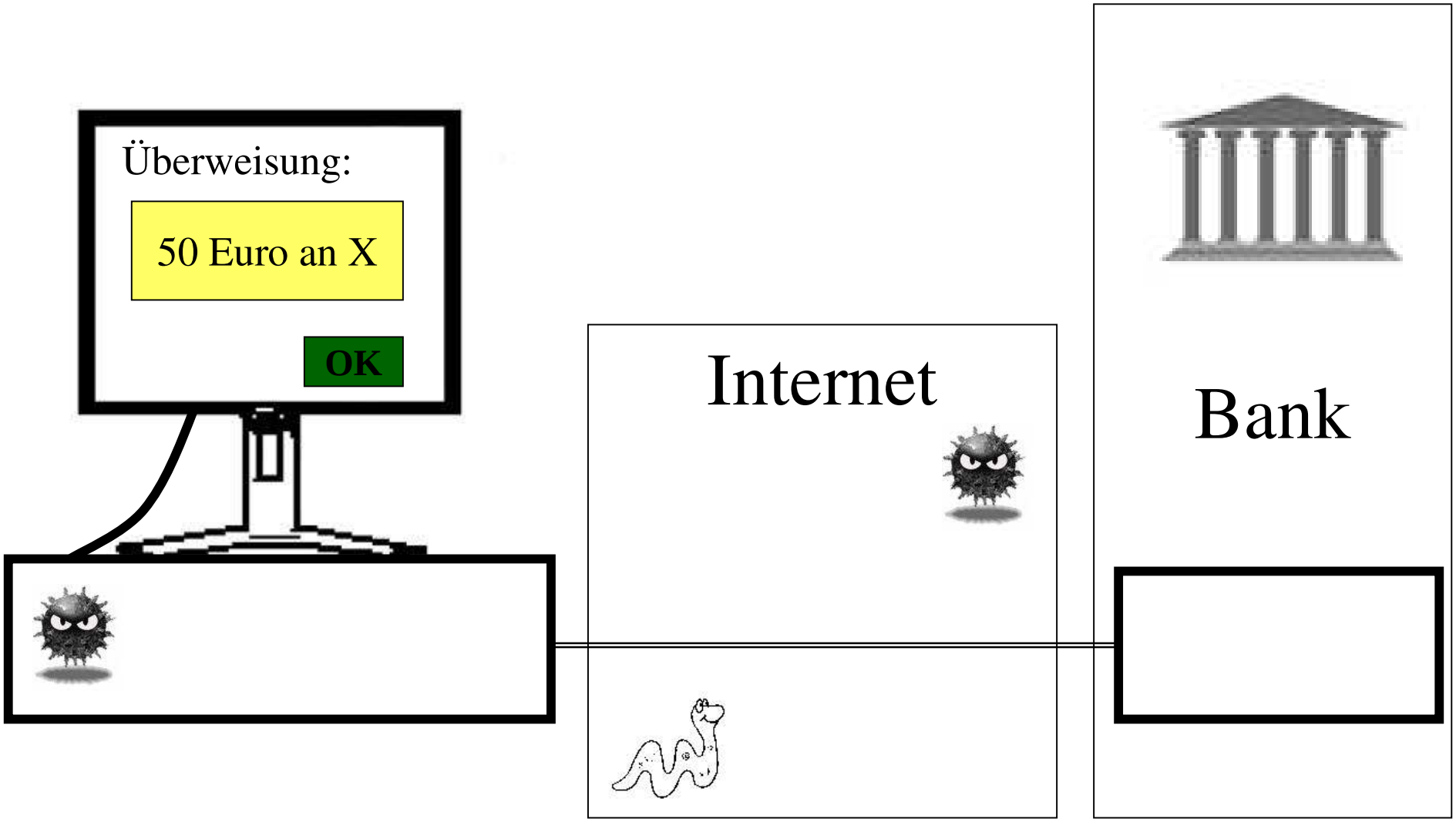

Überweisung:
OK
Internet
Bank



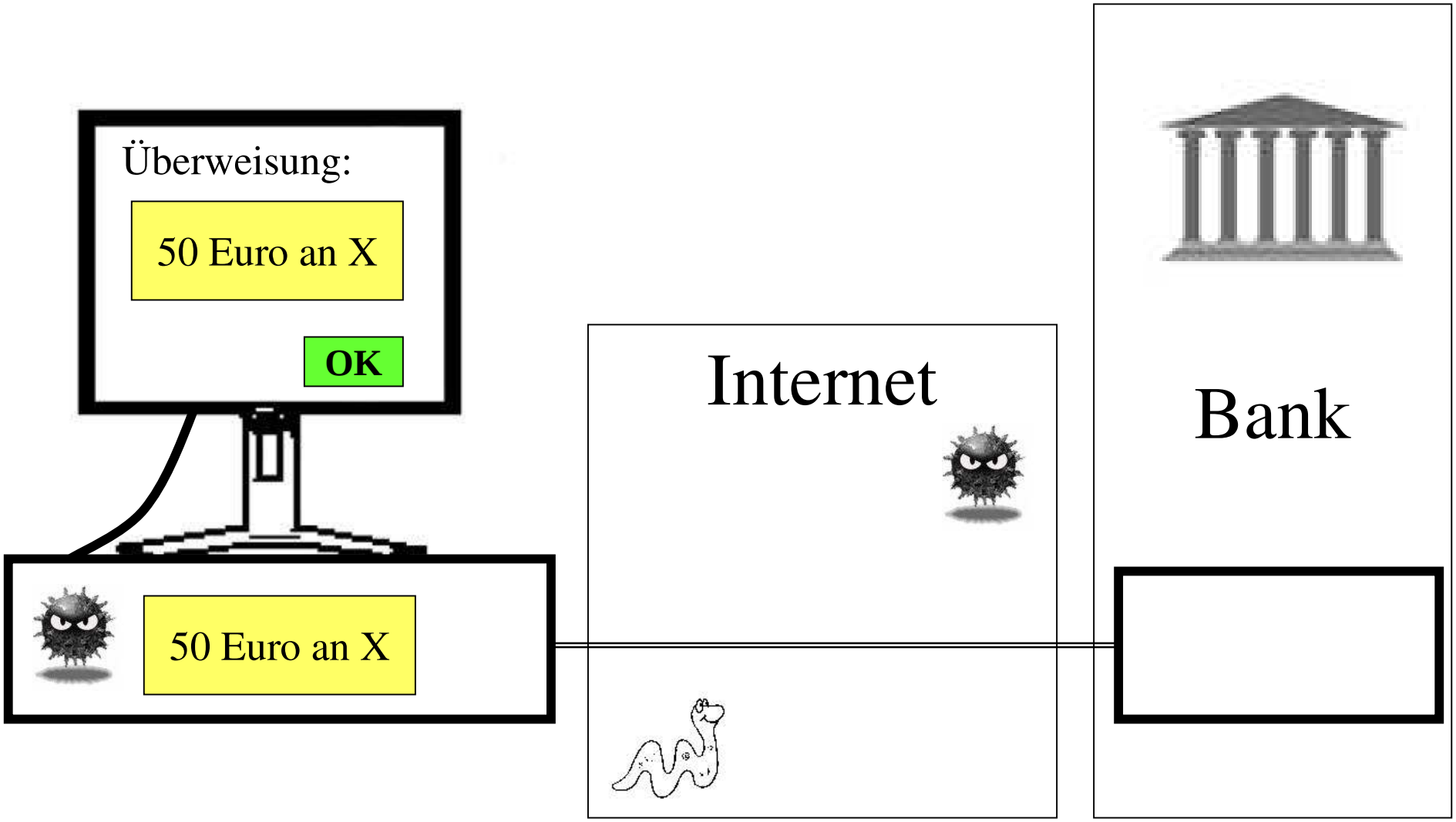
Für die Überweisung wird ein Formular auf den Bildschirm gestellt.



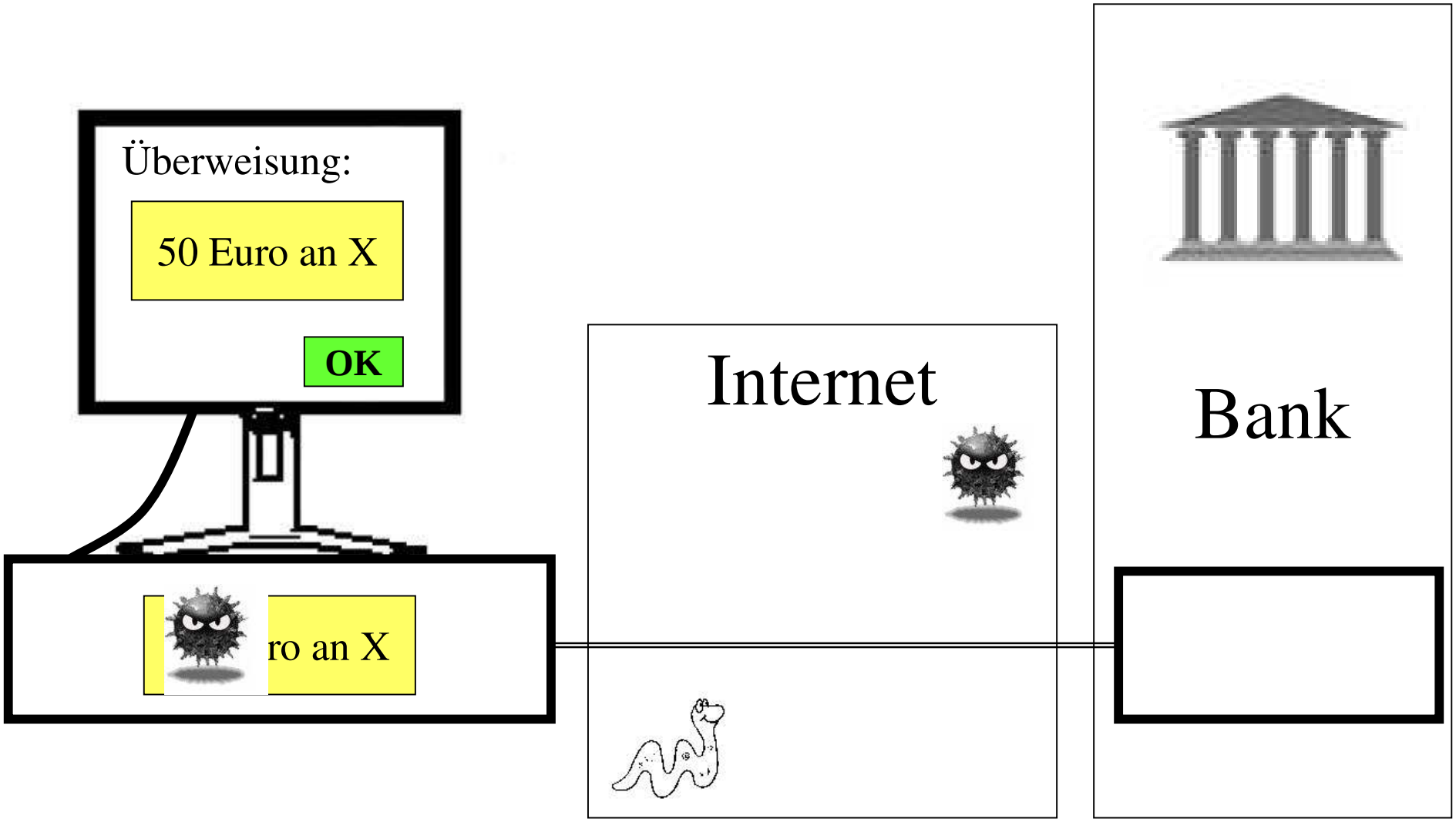
Der Bankkunde füllt das Formular aus.



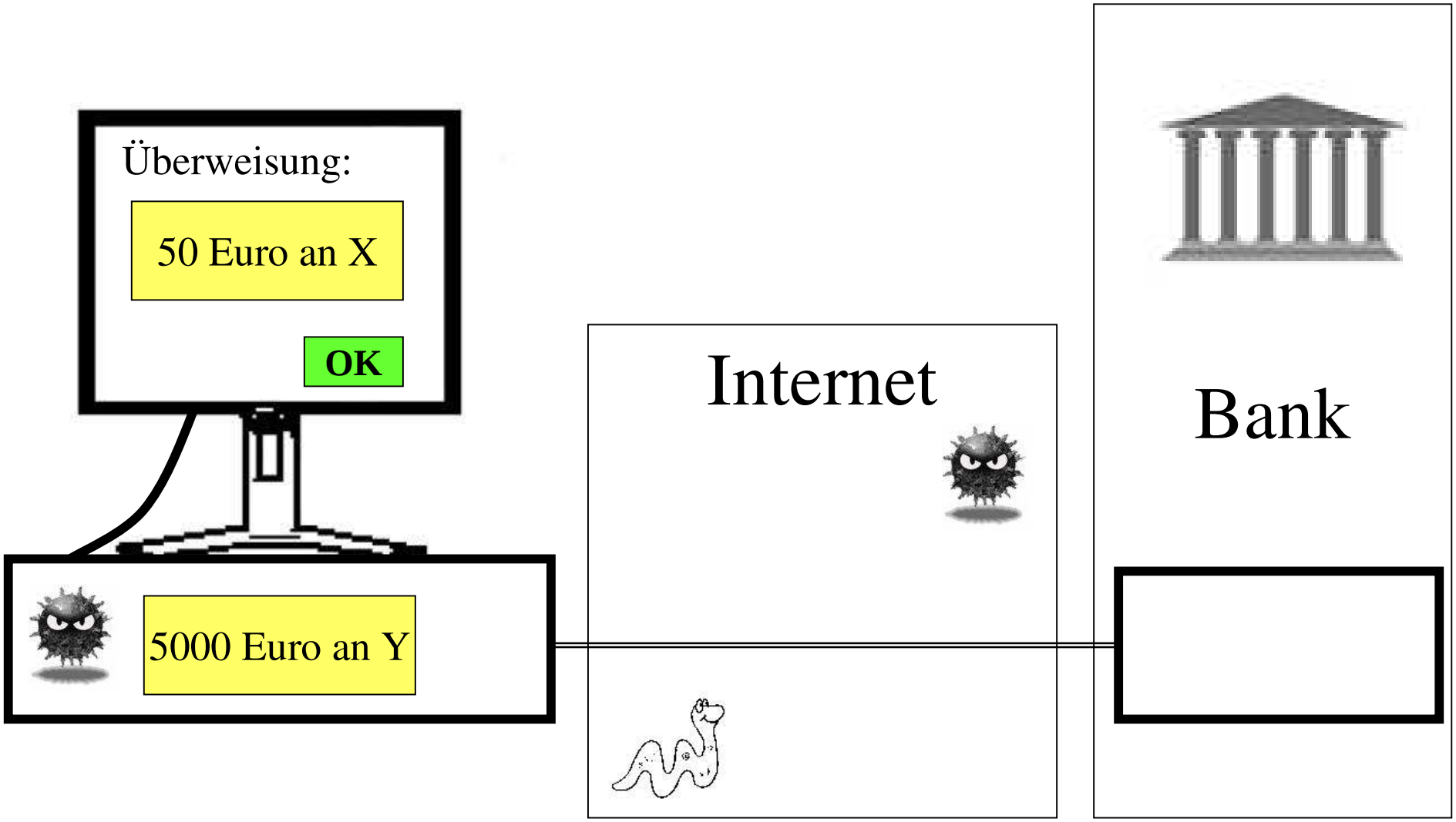
Der Überweisungsauftrag wird „abgeschickt“.



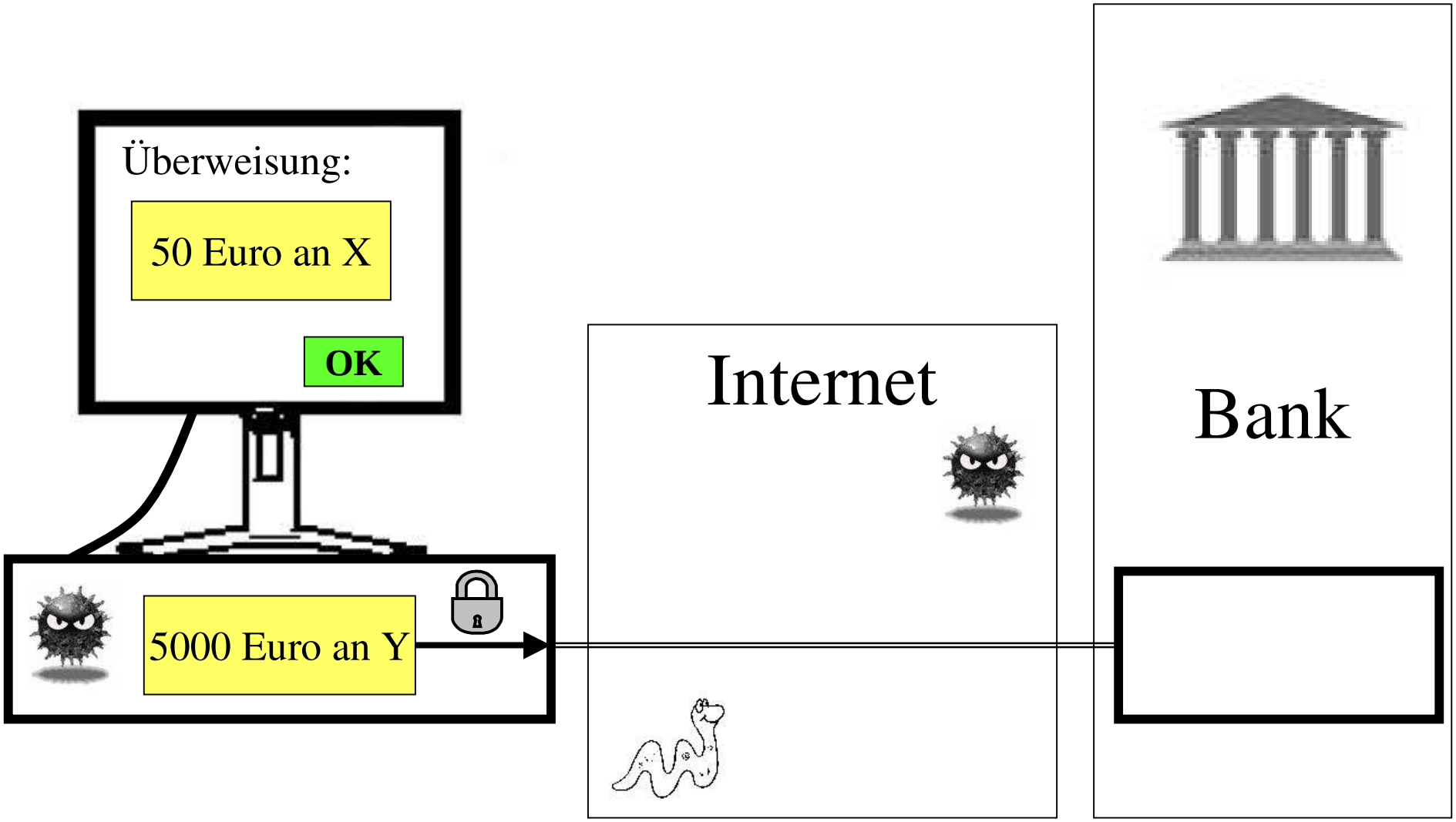
Der Überweisungsauftrag ist noch nicht verschlüsselt.



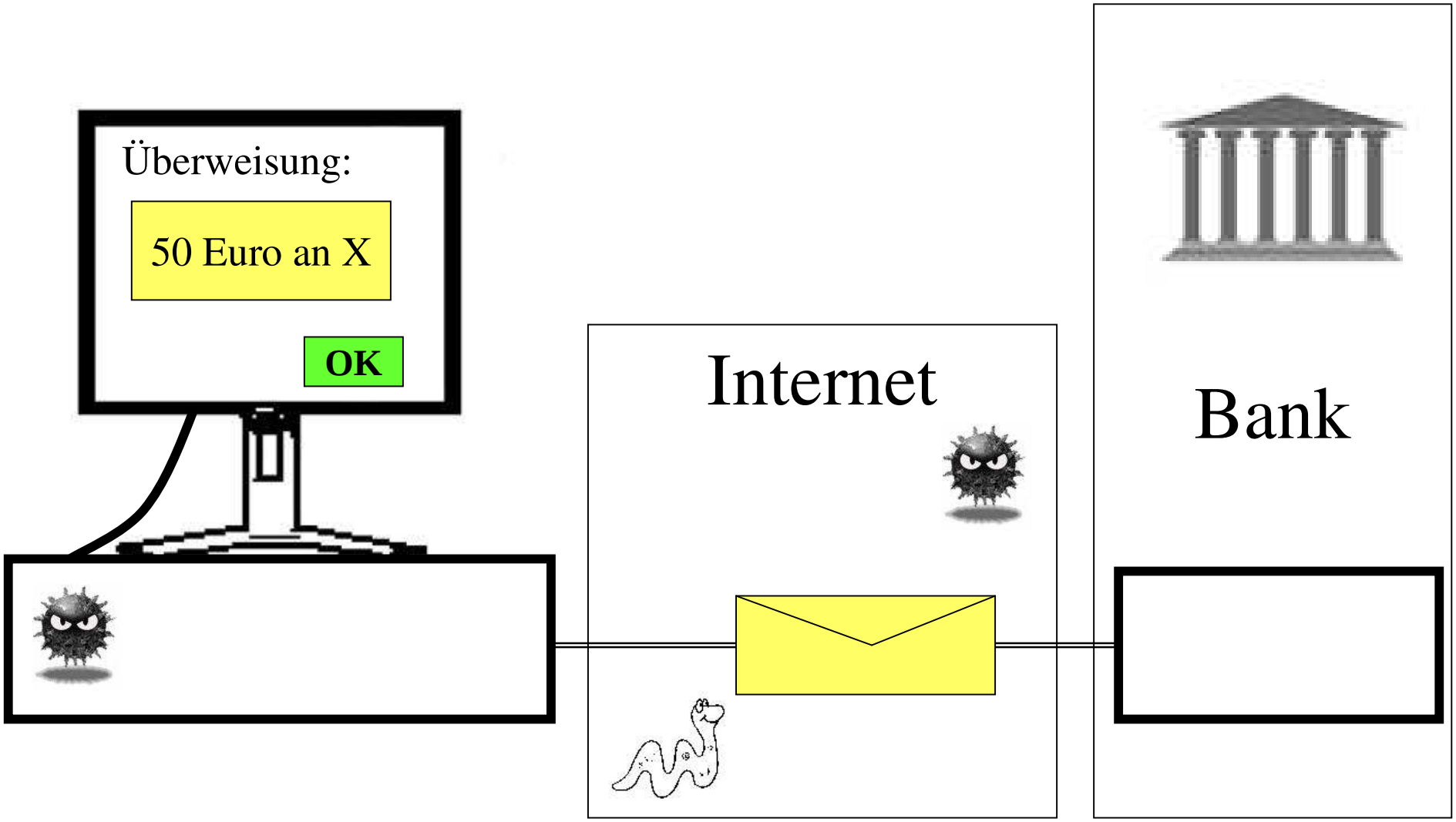
Der Trojaner schaut sich die Überweisungsdaten an ...



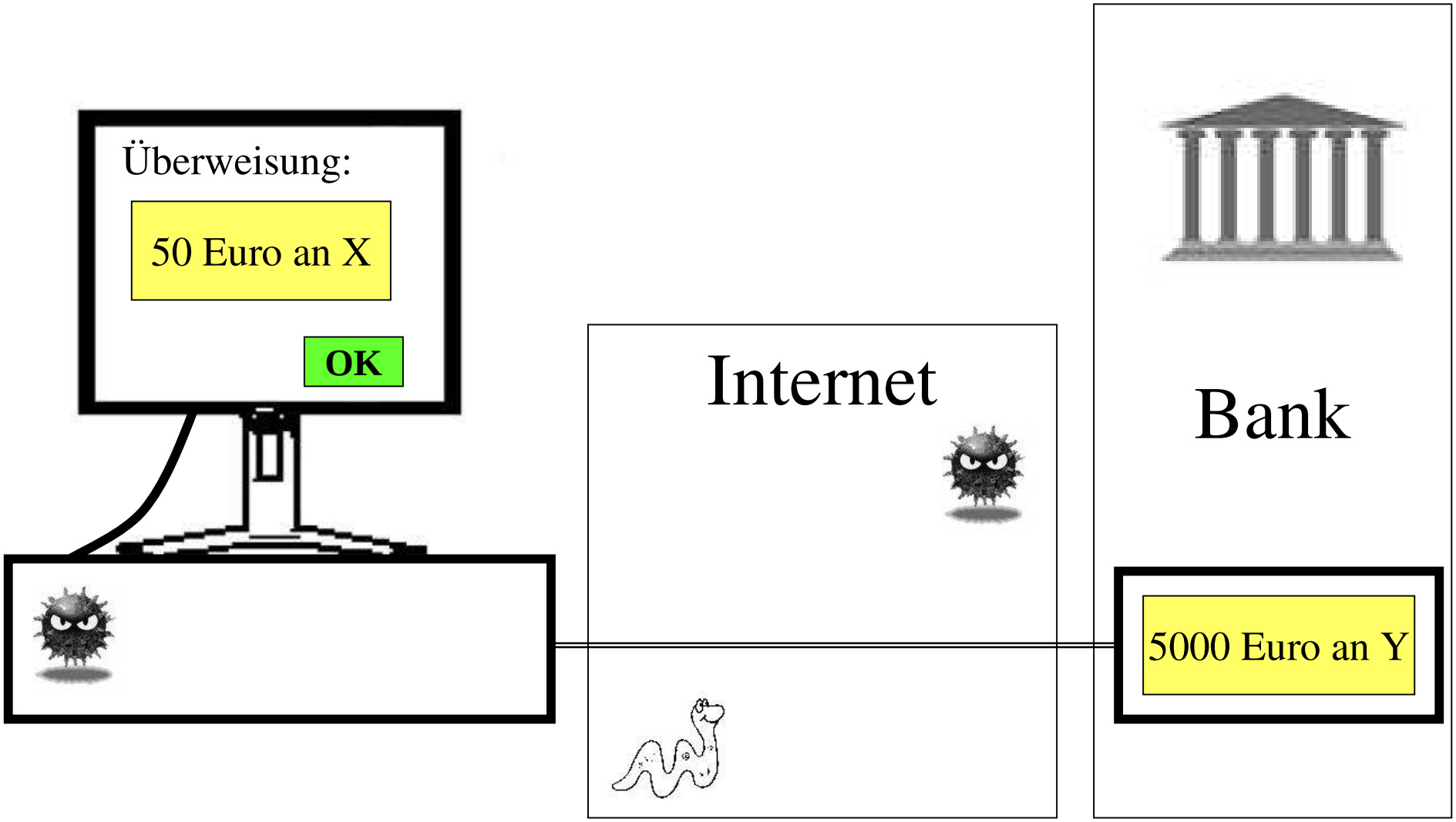
... und fälscht das Zielkonto und den Betrag.



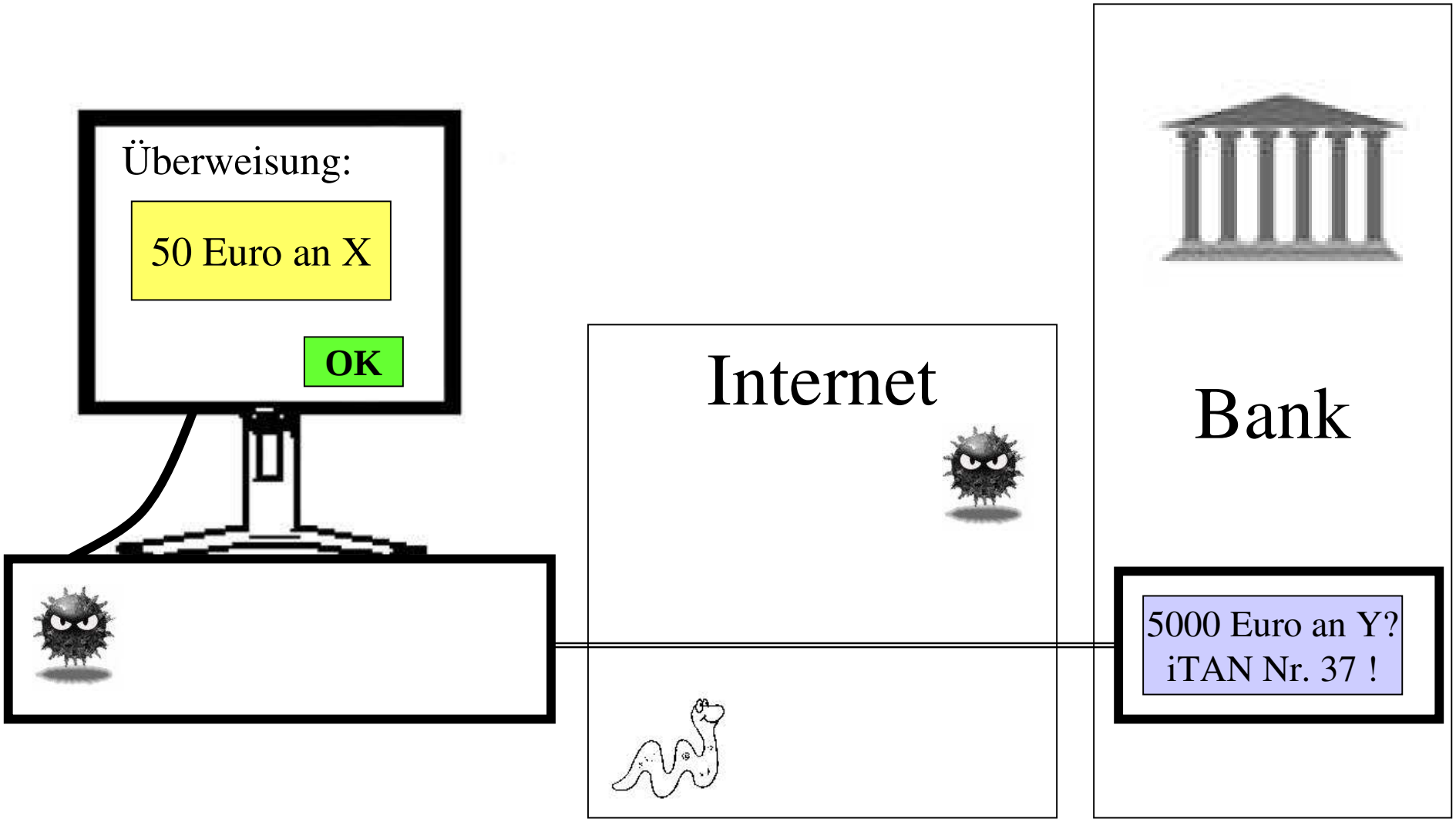
Der gefälschte Überweisungsauftrag wird verschlüsselt ...



... und durch das Internet an den Bank-Server geschickt.

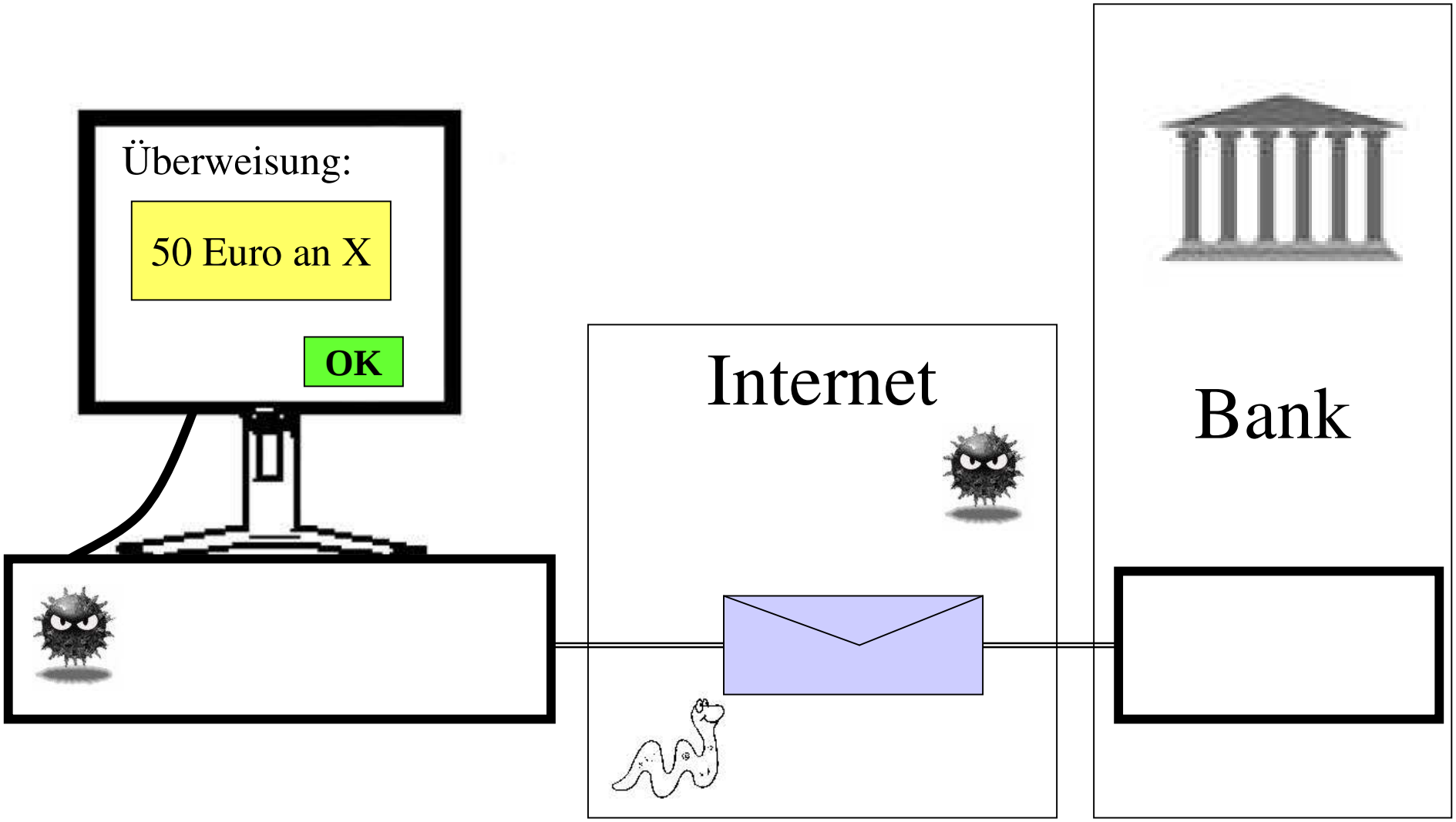


Der Bank-Server entschlüsselt die Nachricht.

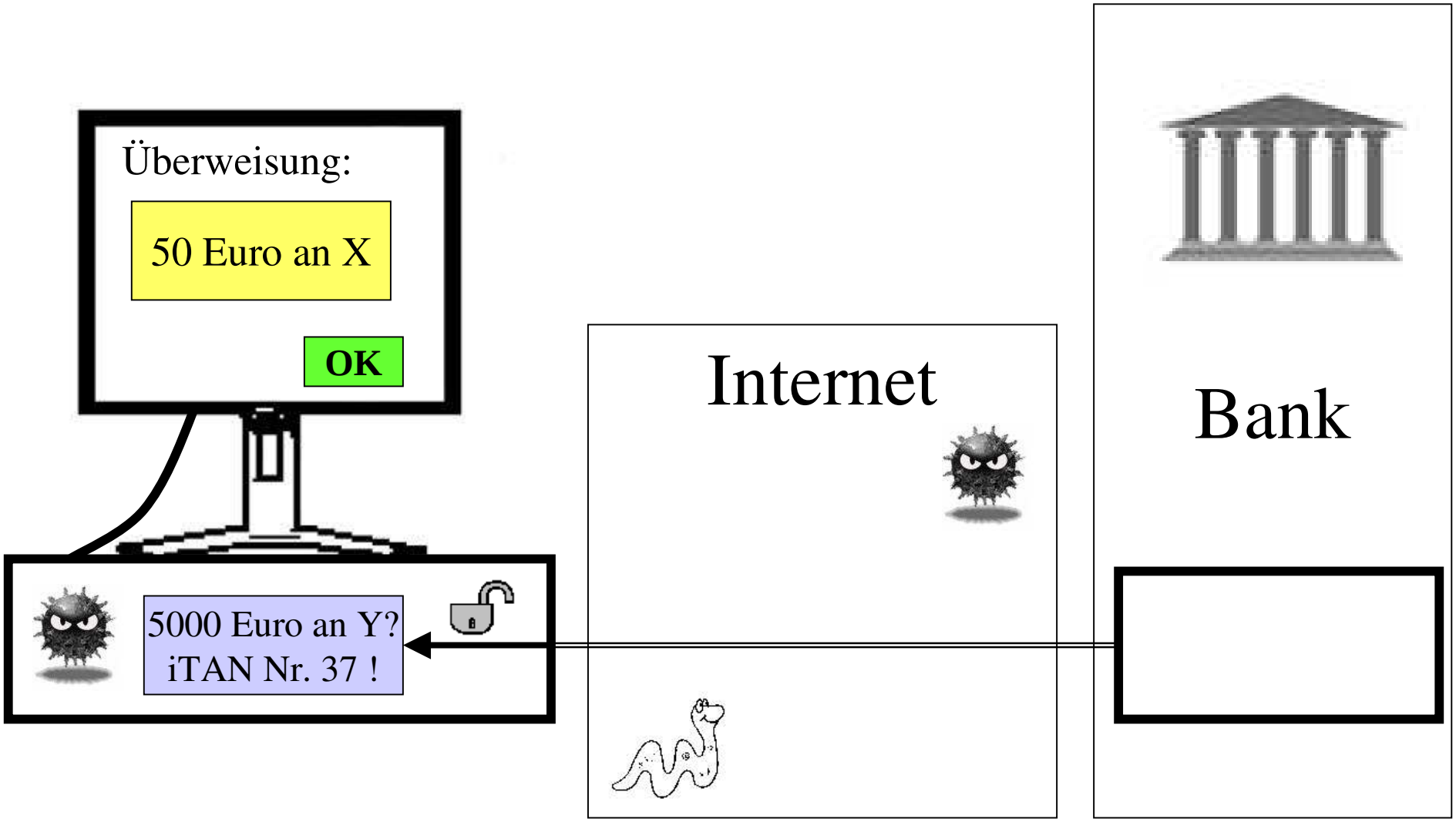


Die Bank kann nicht erkennen, dass der Auftrag gefälscht ist.

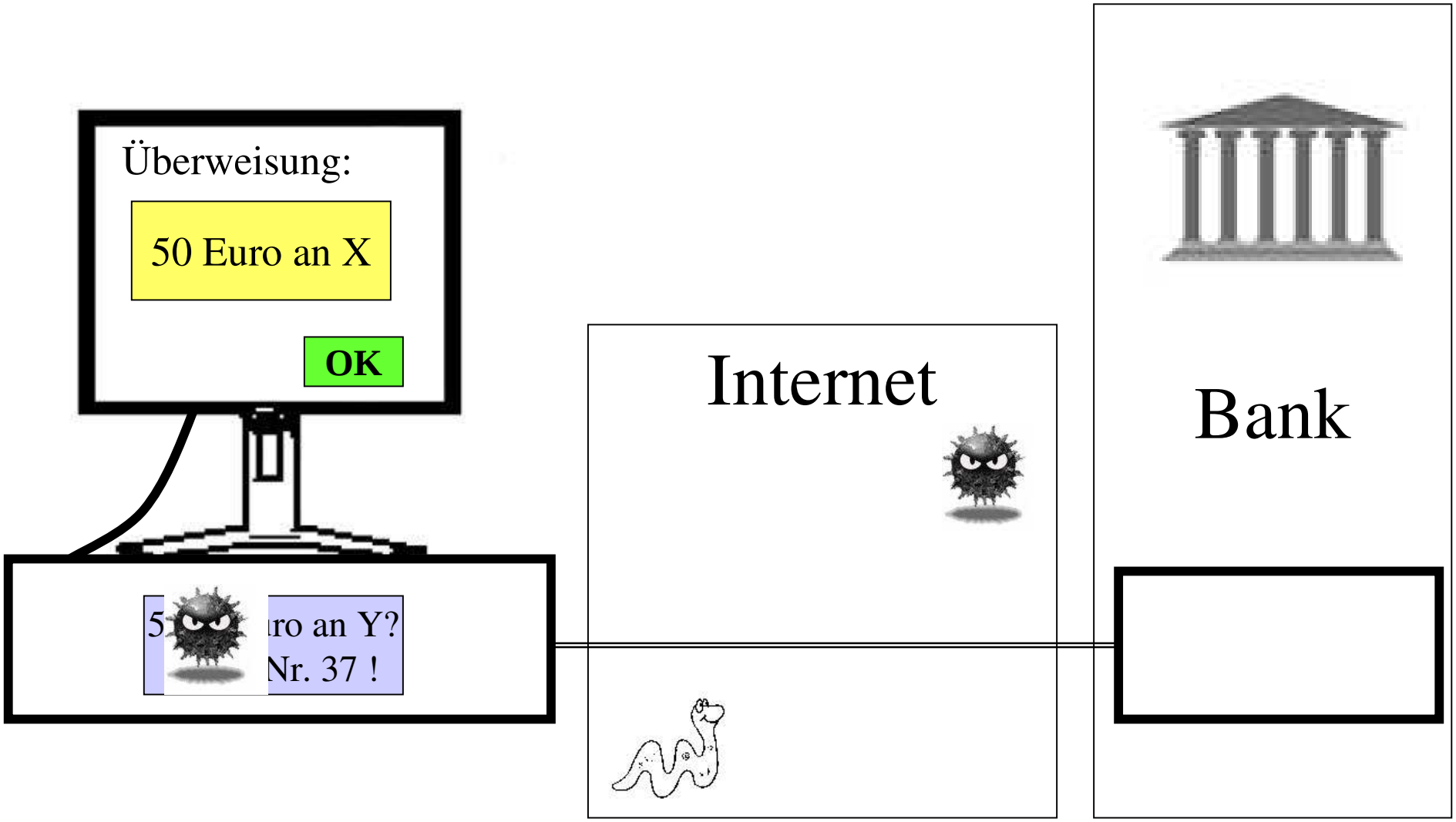
Es wird die iTAN Bestätigungs-Anfrage für den Überweisungsauftrag vorbereitet ...



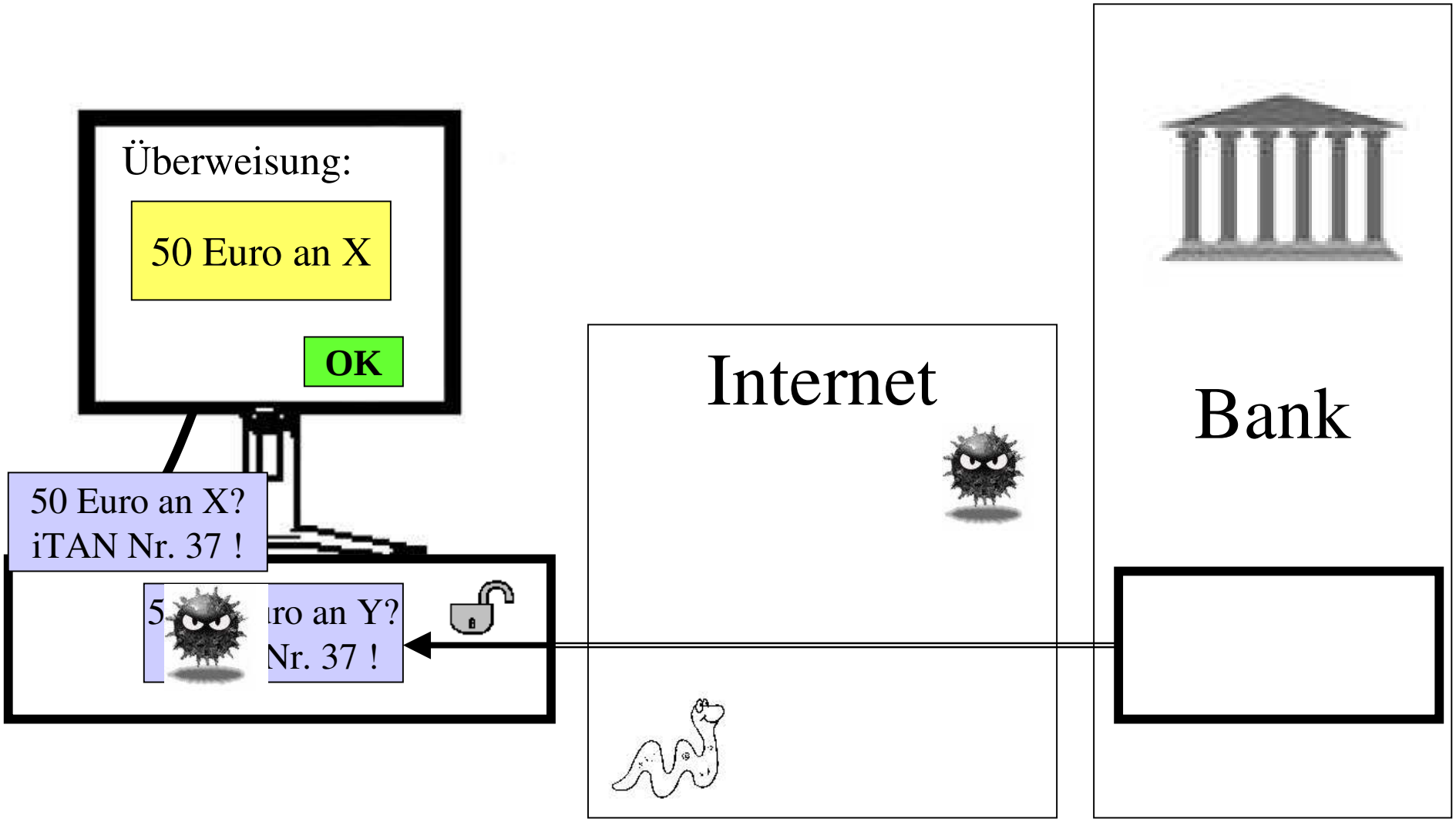
... und verschlüsselt durch das Internet zum Rechner des Bankkunden geschickt.



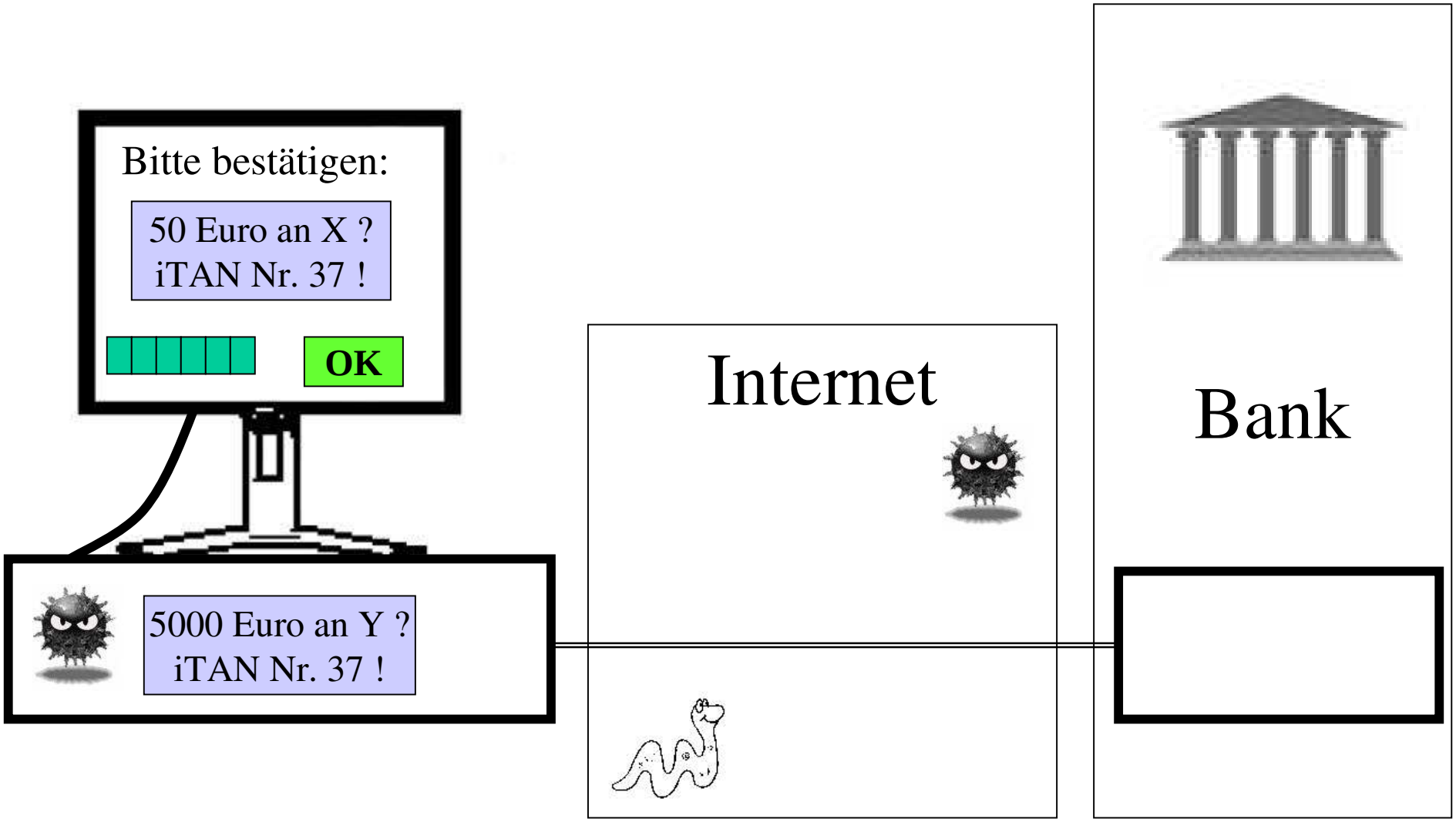
Der Rechner des Bankkunden entschlüsselt die iTAN Bestätigungs-Anfrage.



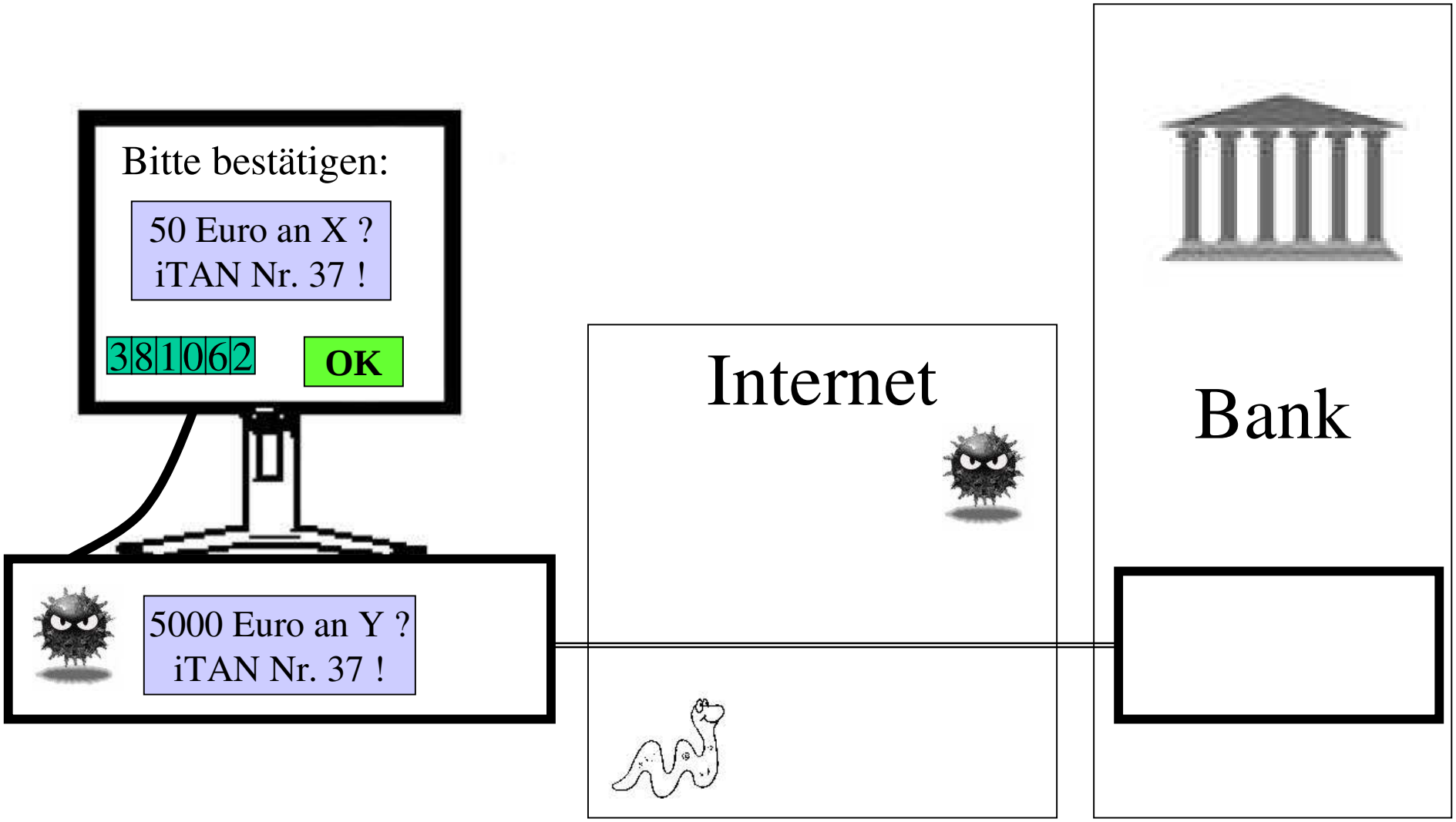
Der Trojaner-Virus liest die Nachricht ...



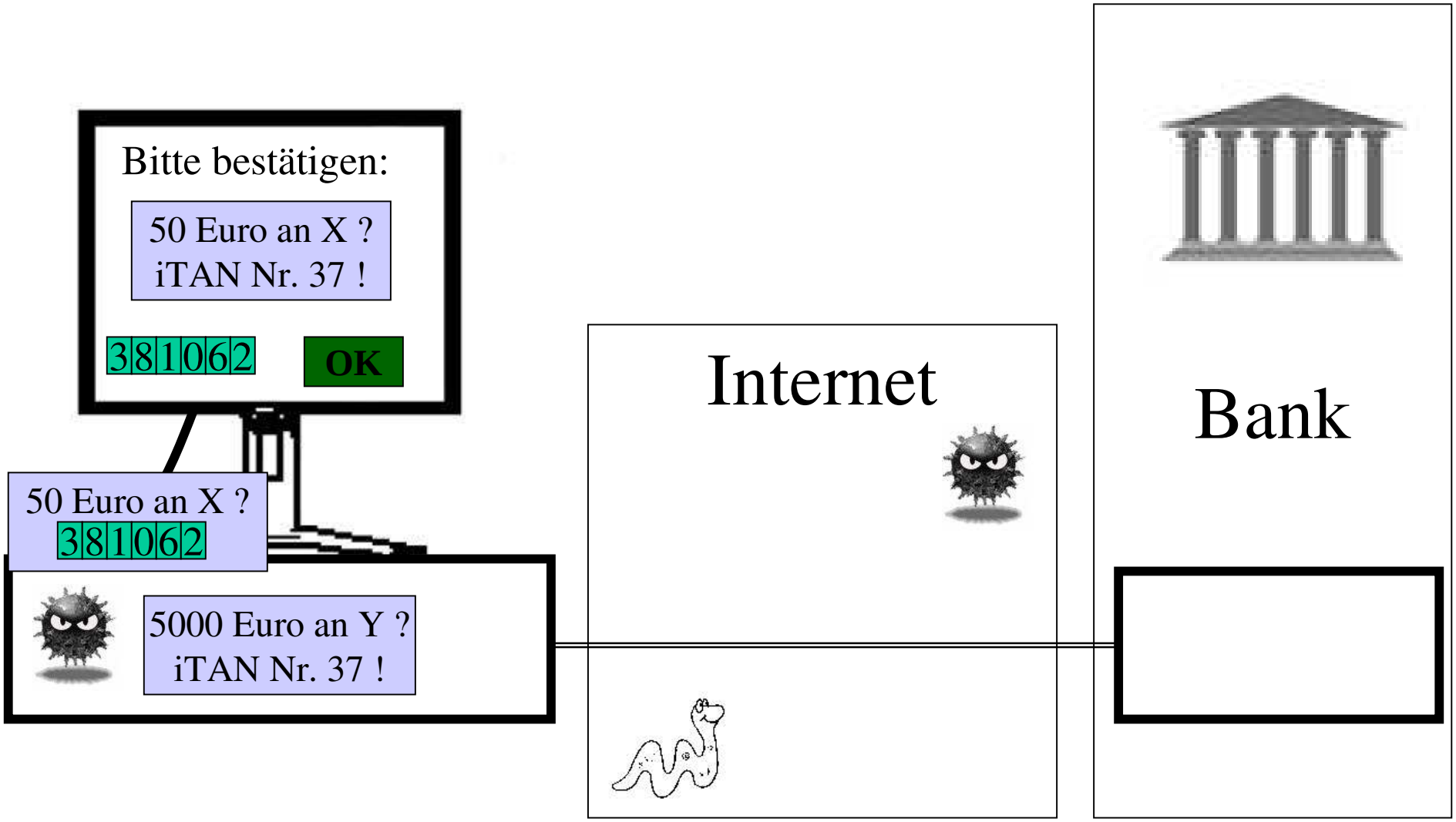
... und fälscht sie ab, und zwar so, dass die vom Bankkunden ursprünglich eingegebenen Daten zu erkennen sind. Die nachgefragte iTAN Nummer (hier Nr. 37) bleibt.



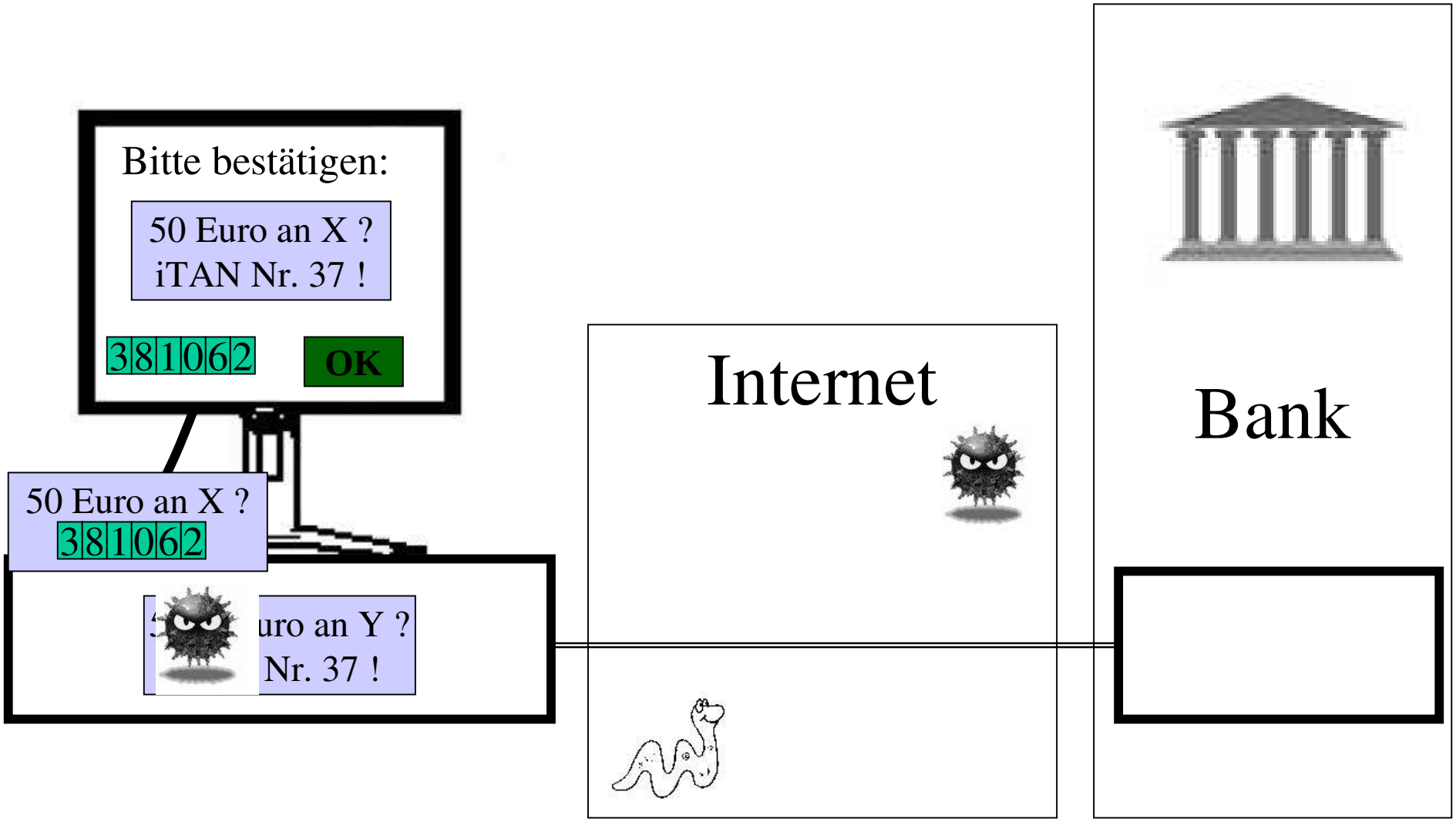
Die zurück-gefälschte iTAN Bestätigungs-Anfrage wird auf dem Bildschirm dargestellt.



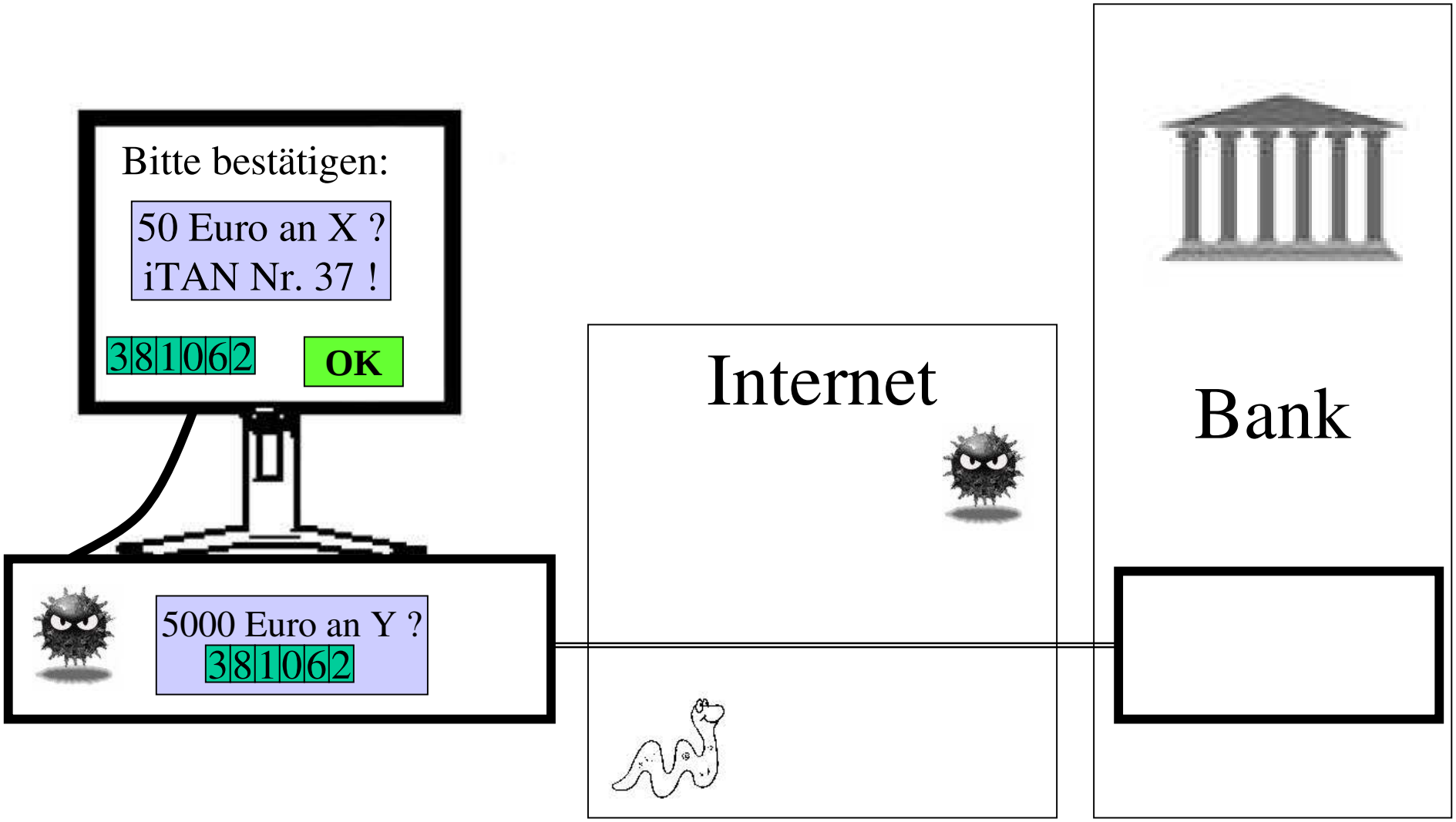
Der ahnungslose Bankkunde gibt die angefragte iTAN ein.



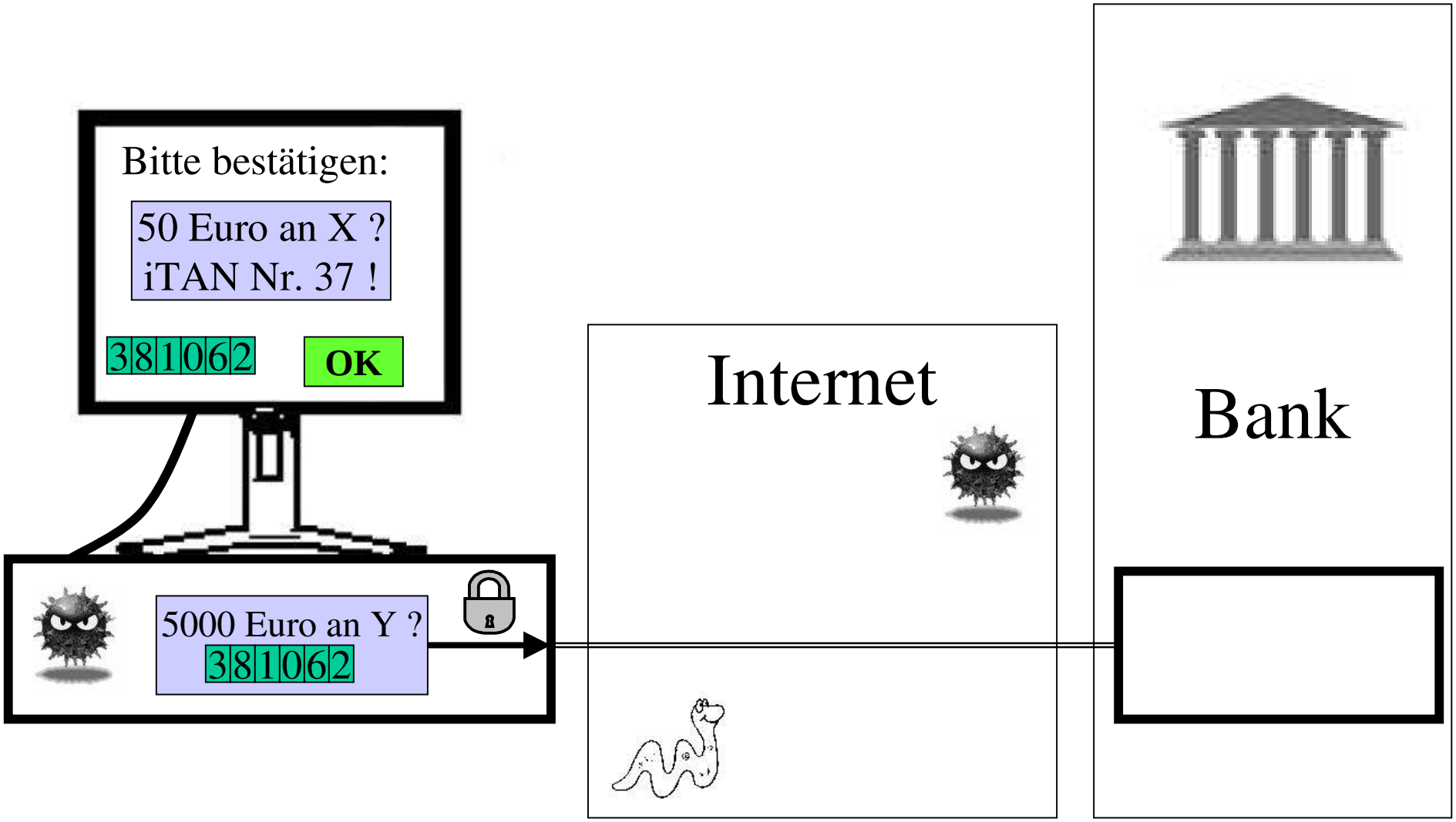
Die iTAN wird vom Bankkunden „abgeschickt“.



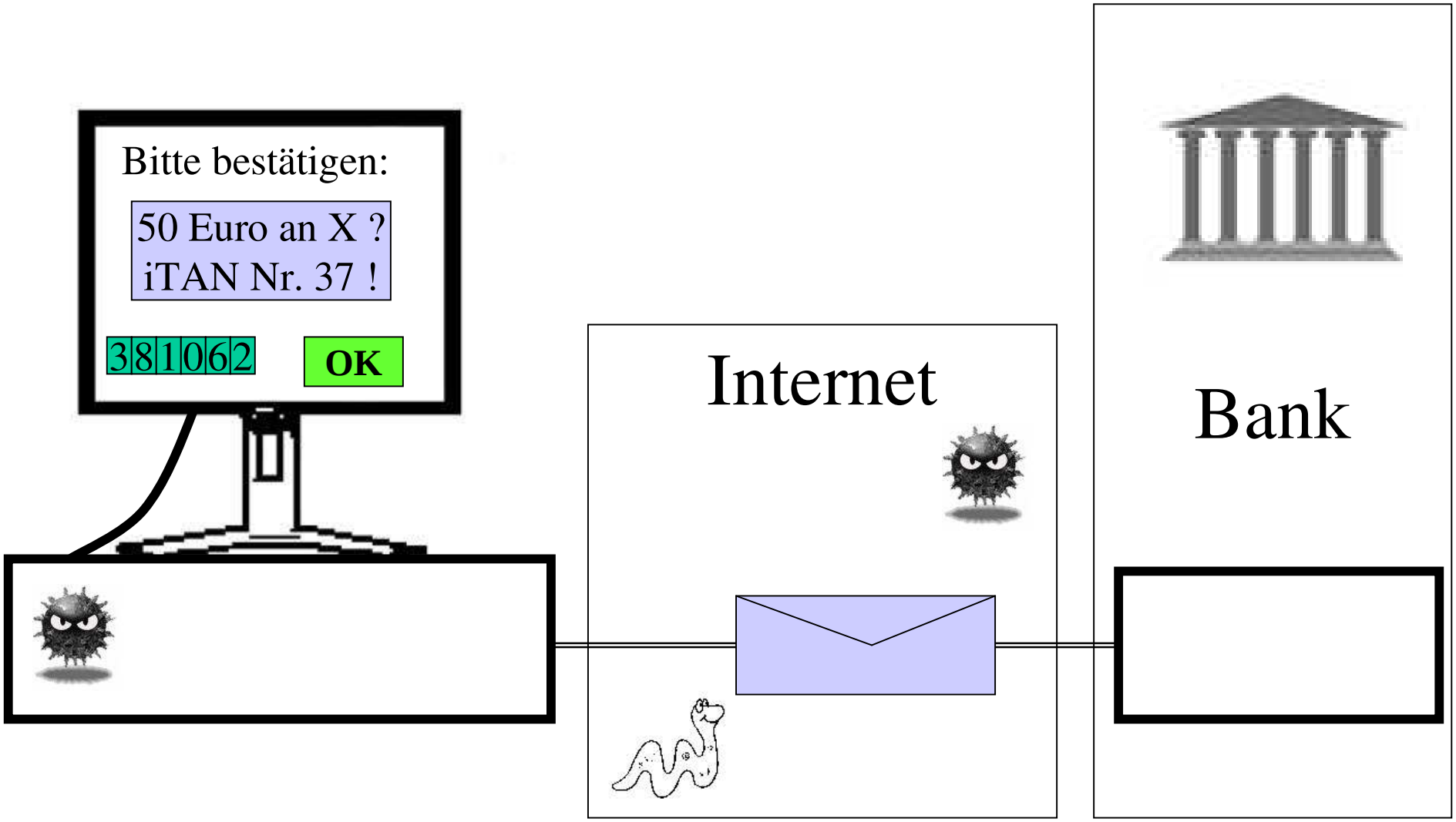
Der Trojaner nimmt die von Bankkunden eingegebene iTAN ...



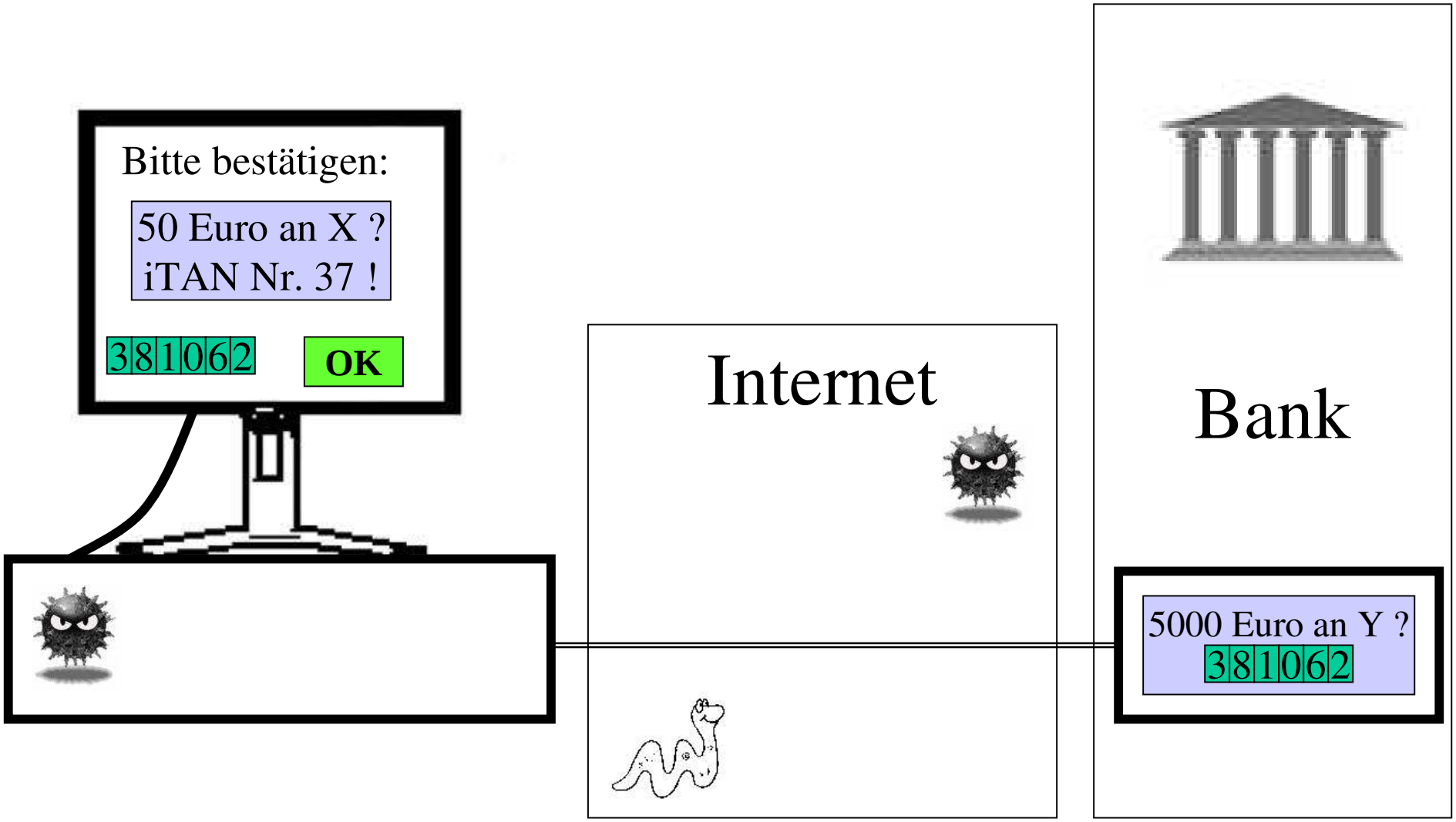
... und nutzt sie als iTAN für die gefälschten Überweisungsdaten.



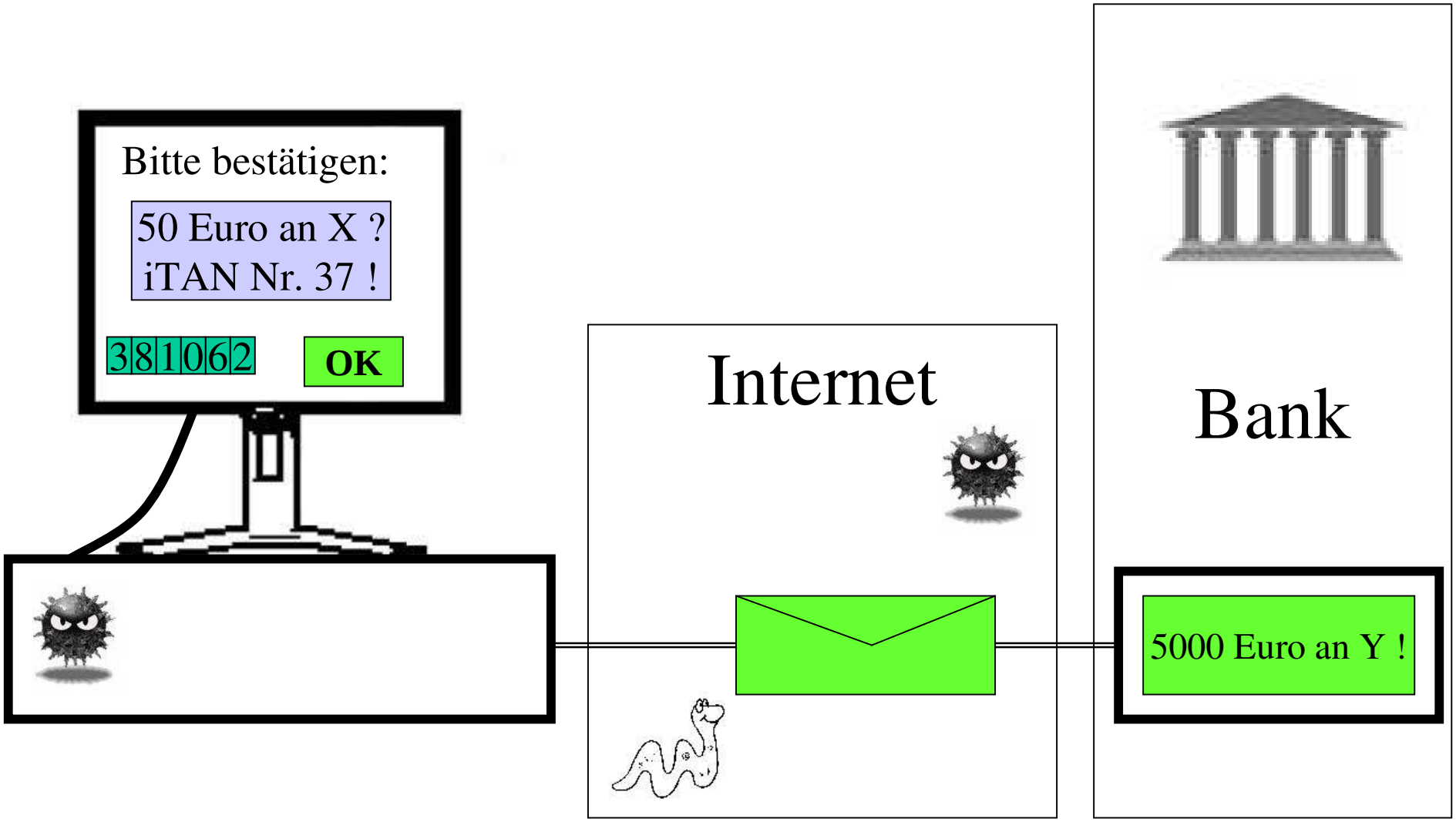
Das wird verschlüsselt ...



... und durch das Internet zum Bank-Server geschickt.

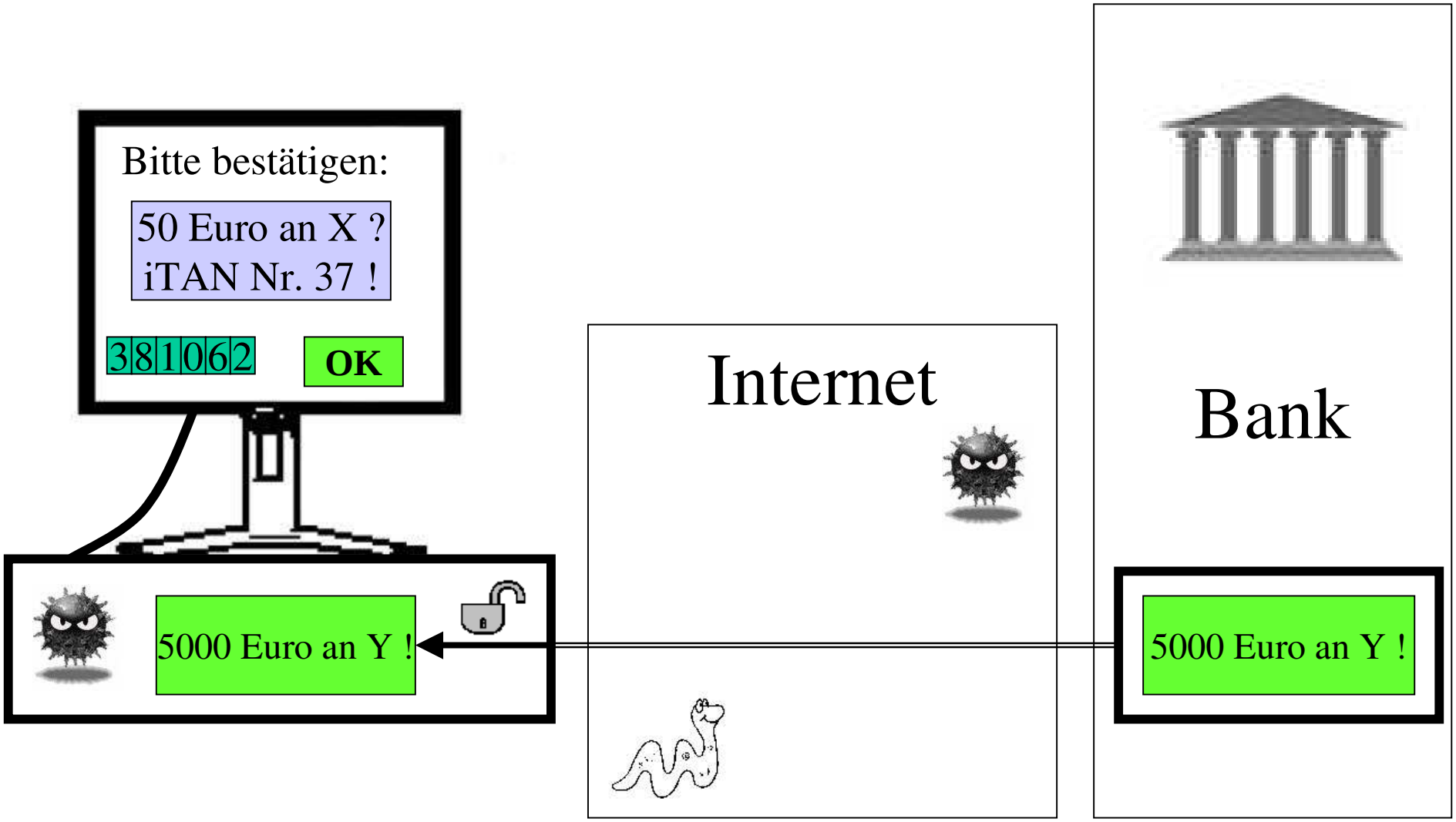


Der Bank-Server entschlüsselt die Nachricht und überprüft die Richtigkeit der iTAN.

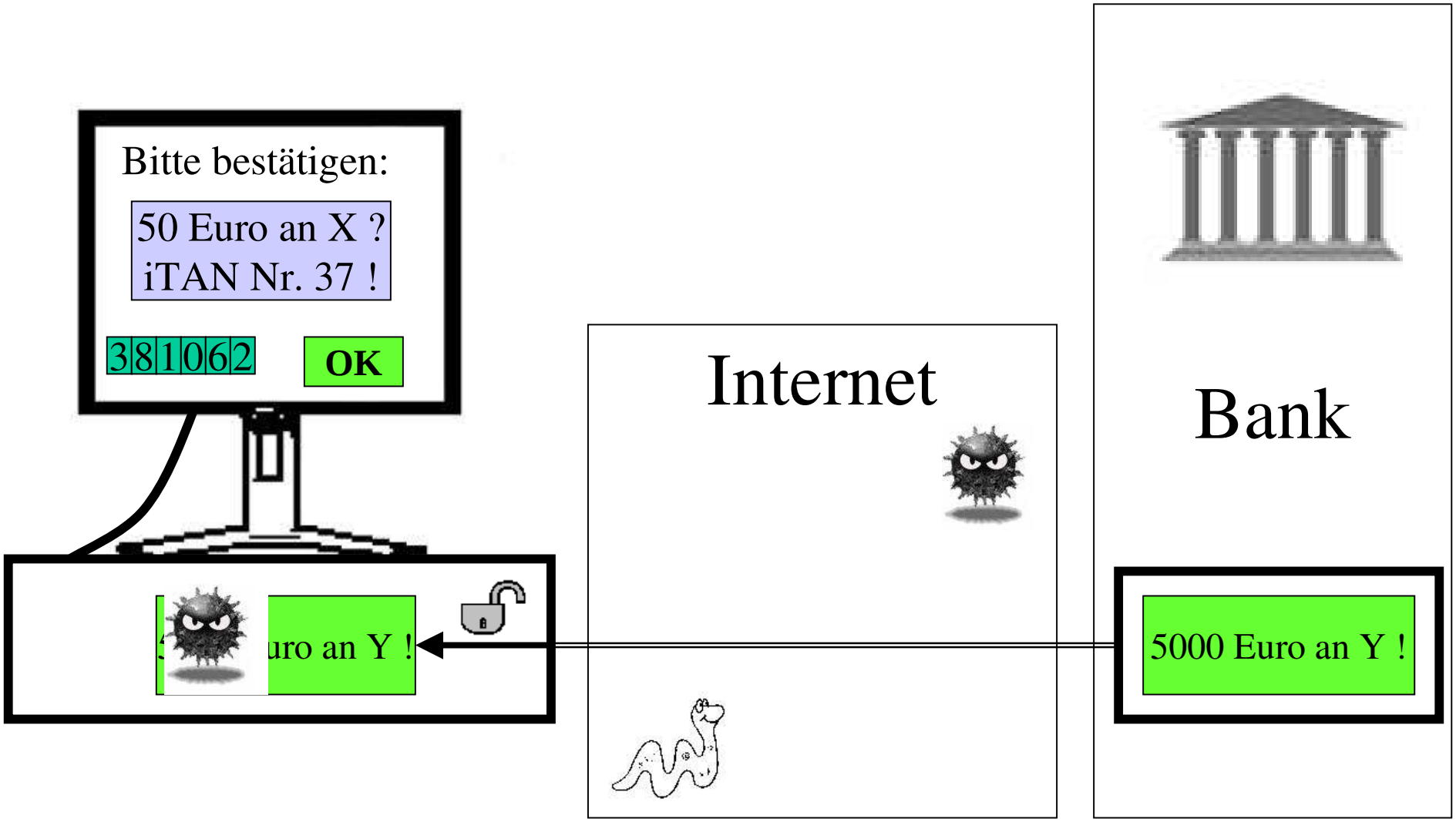


Weil die iTAN korrekt ist, wird der gefälschte Auftrag angenommen.

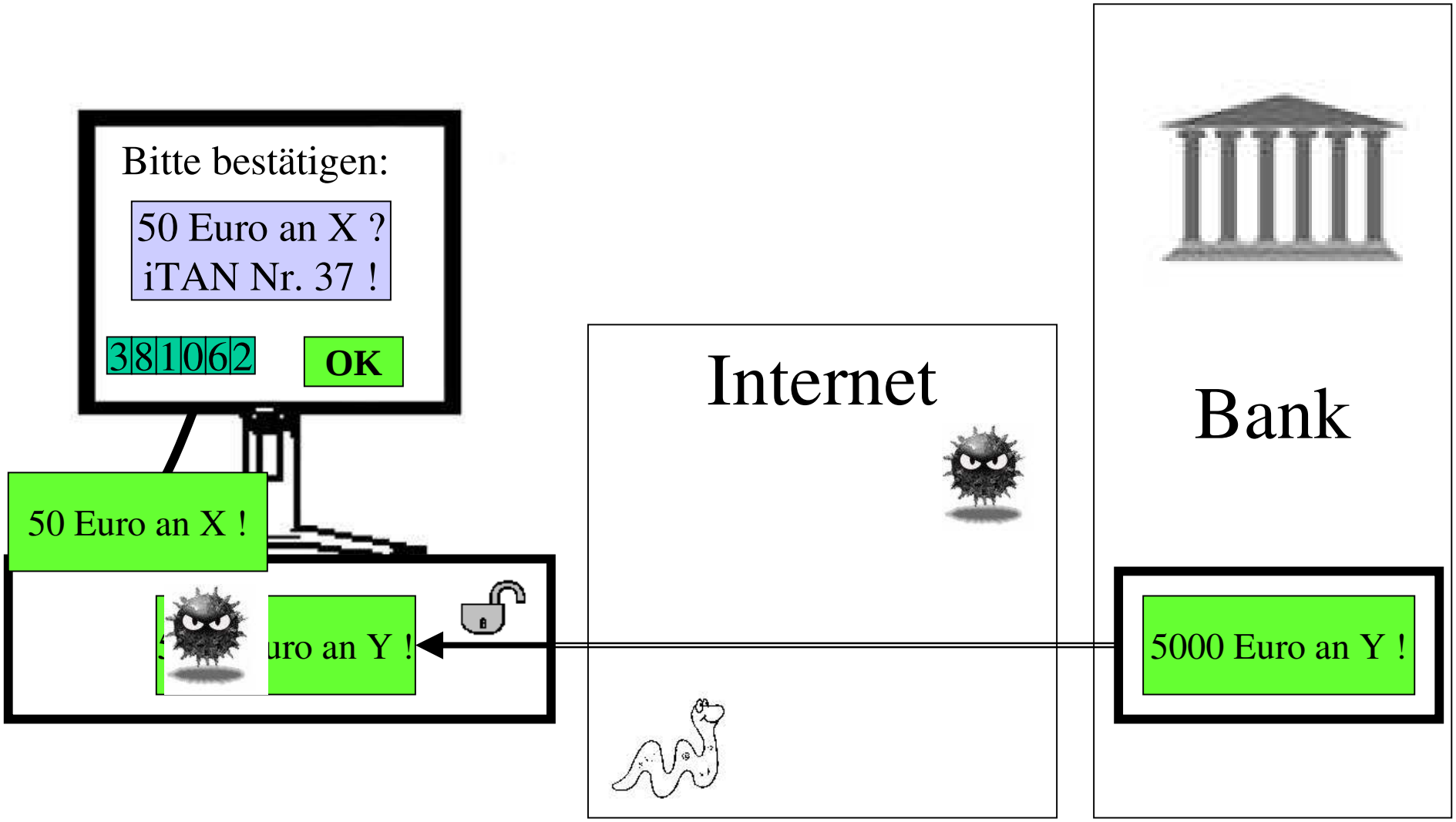
Ausserdem wird noch die Bestätigung zum Bankkunden geschickt.



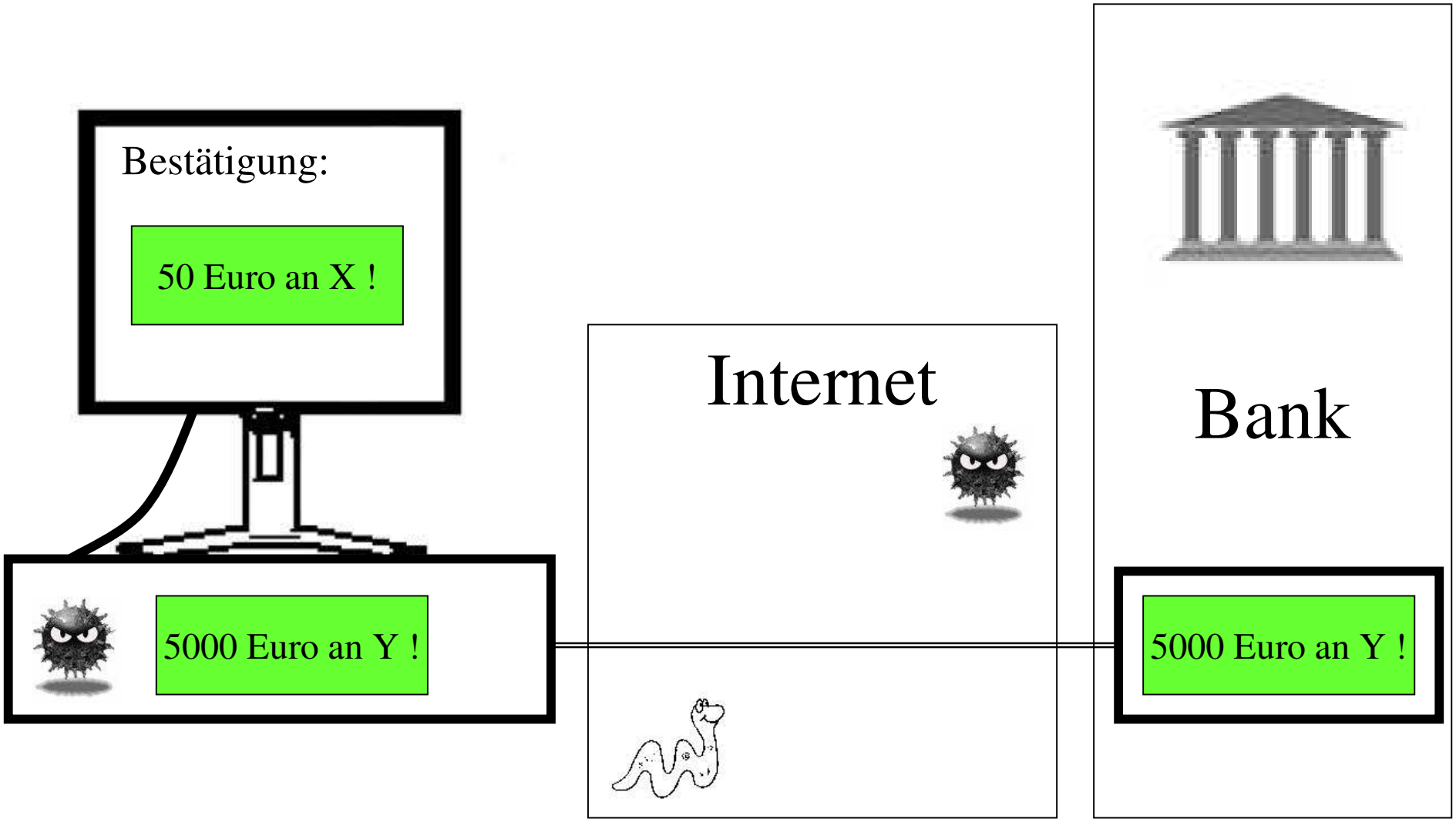
Die Bestätigung wird entschlüsselt ...



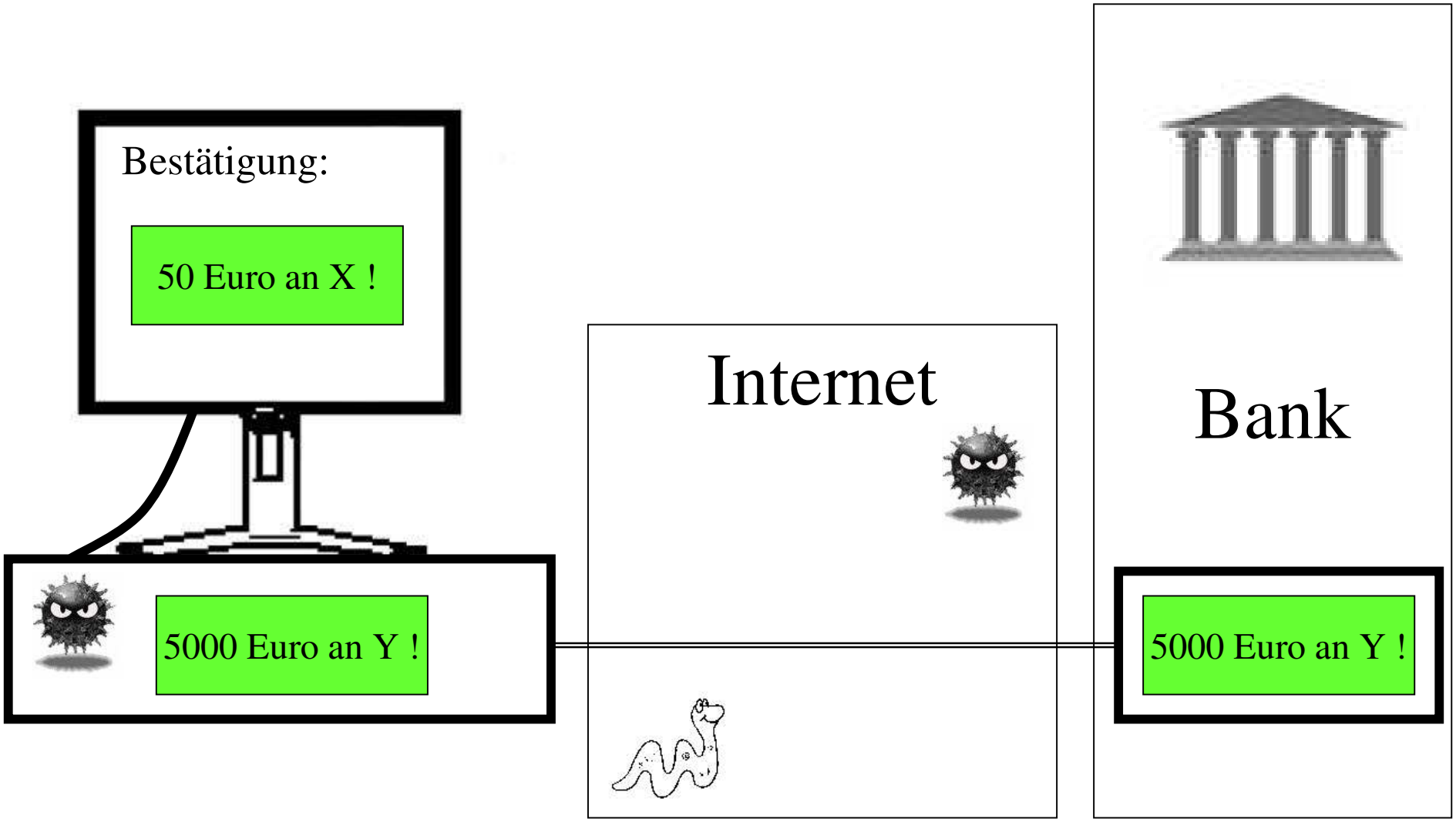
... vom Trojaner-Virus gelesen ...



... und „korrigiert“.

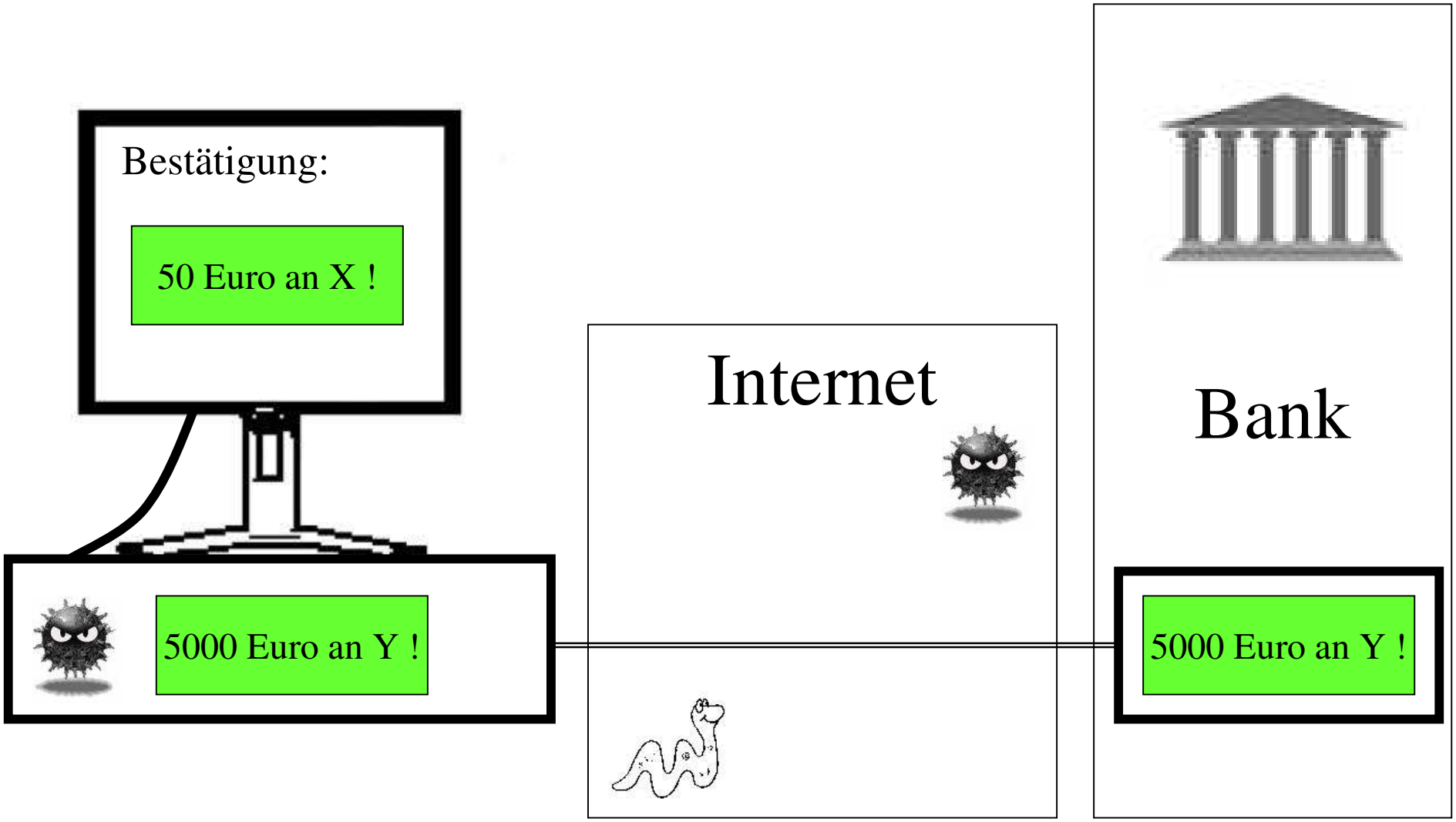


Der Benutzer sieht die von ihm eingegebenen Überweisungsdaten bestätigt.

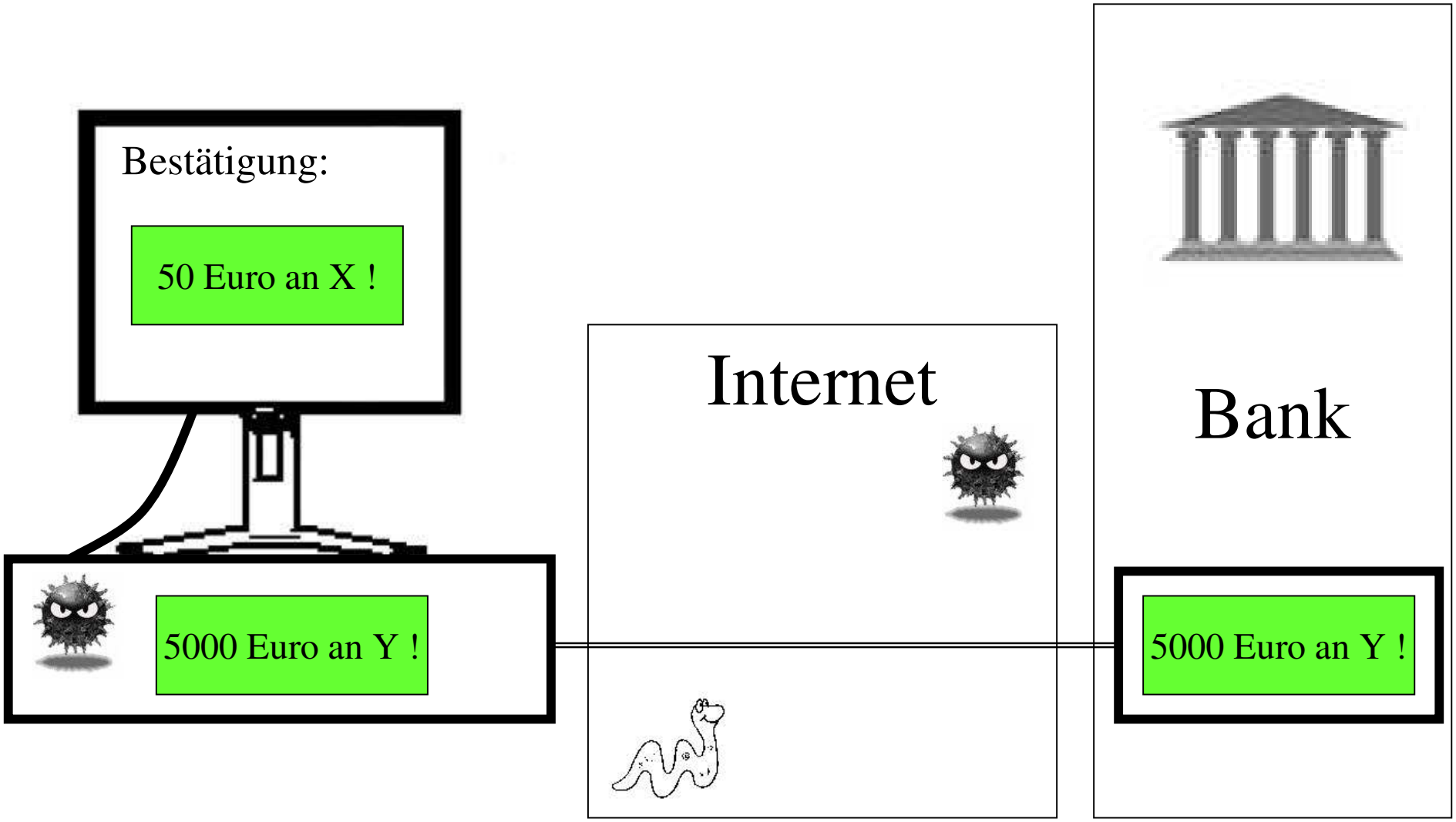


Die Bank hat den gefälschten Auftrag ausgeführt!

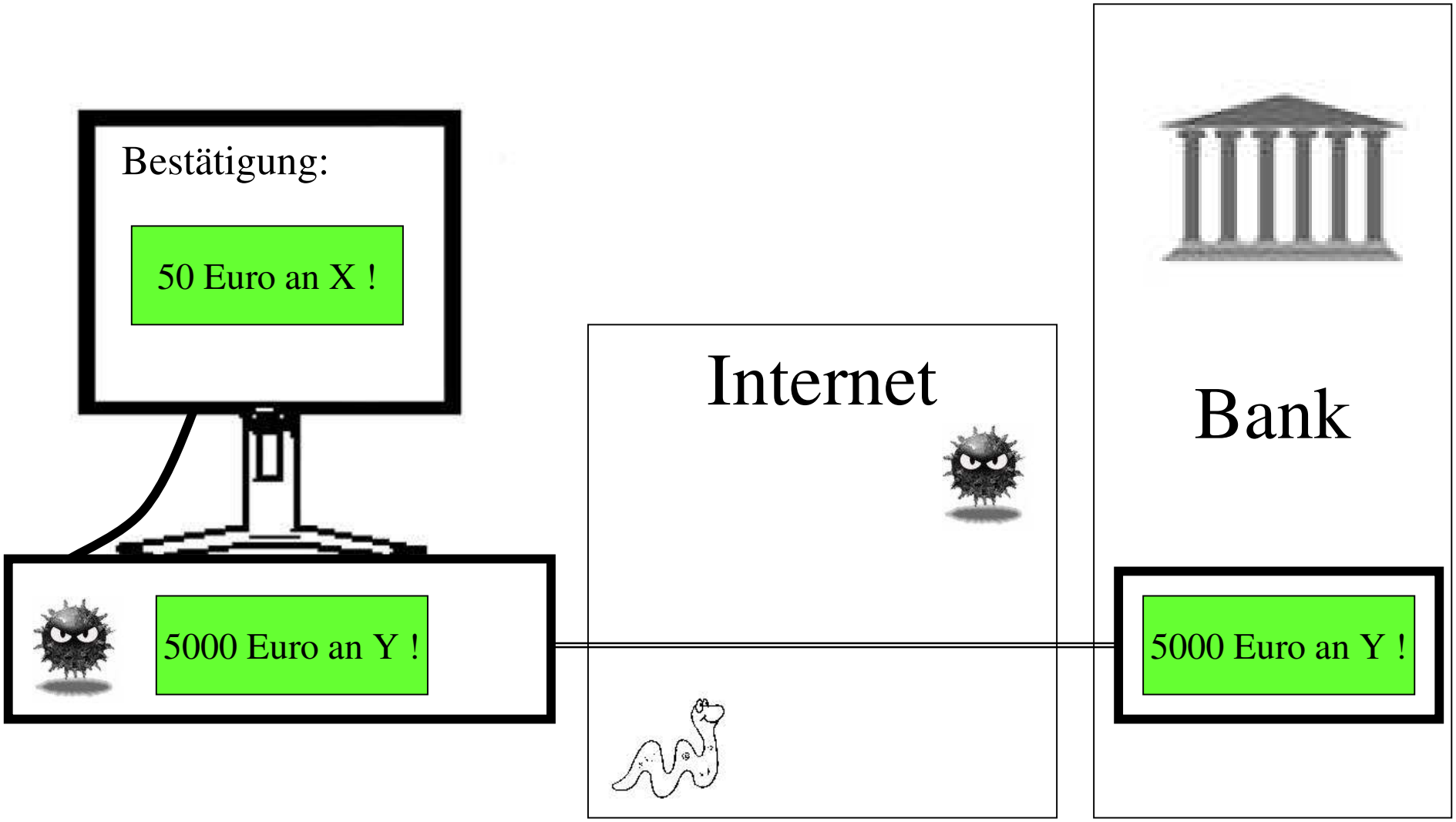
Weder der Bankkunde noch der Bank-Server haben die Betrug bemerkt.



Der Bankkunde und die Bank sind vom Trojaner-Virus reingelegt worden.



Der Trojaner-Virus freut sich hämisch ...


Bestätigung:
50 Euro an X !
Internet
Bank
5000 Euro an Y !
5000 Euro an Y !

Das war‘s.