

# POLITECHNIKA ŚWIĘTOKRZYSKA

## LABORATORIUM CYBERBEZPIECZEŃSTWO

Numer ćwiczenia:

3

Temat ćwiczenia:

Dostęp do plików poufnych

Damian Zdyb

Data wykonania:

23.11.2018

Data oddania do sprawdzenia:

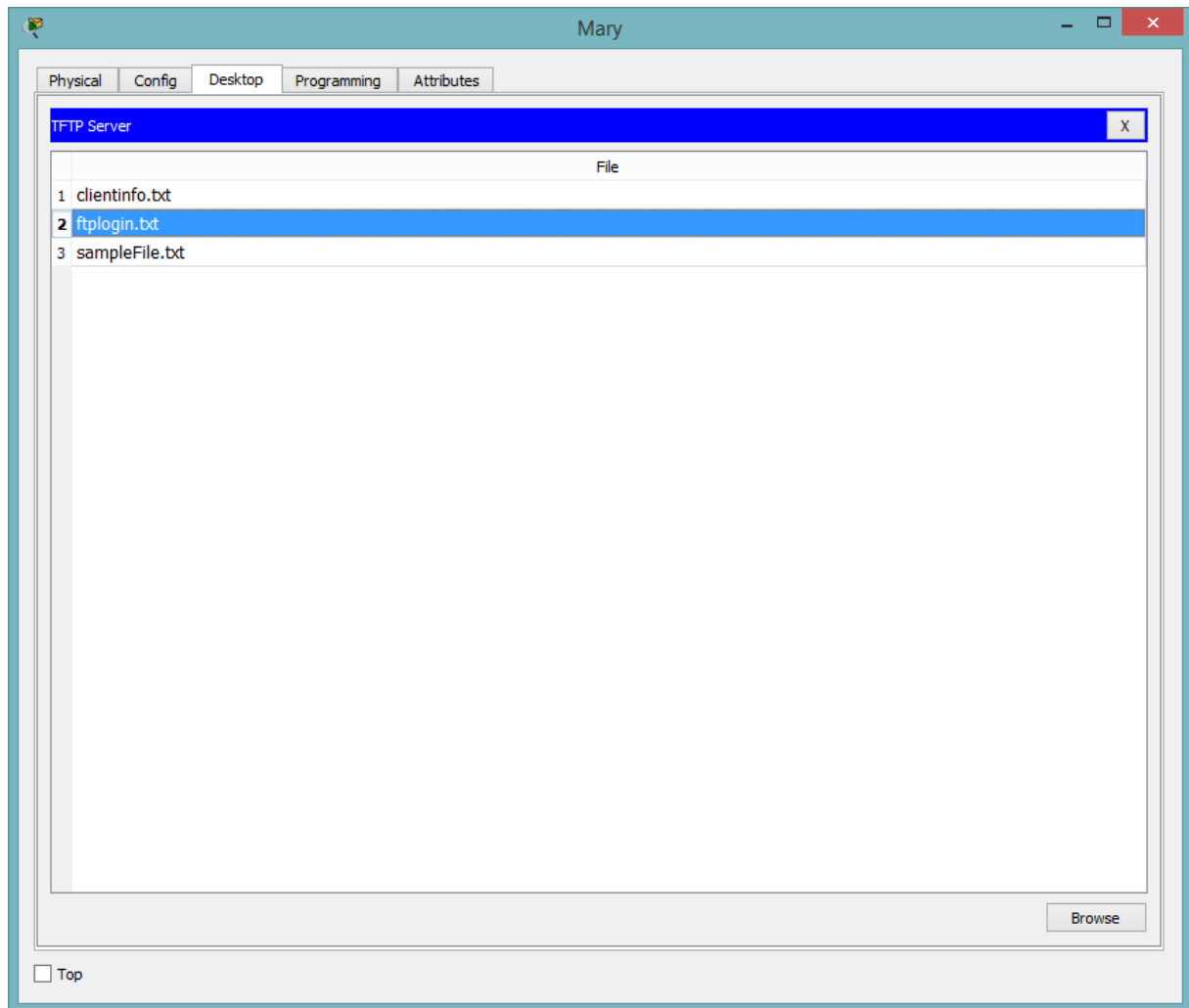
24.11.2018

Ocena:

## Część 1: Zlokalizuj dane logowania na konto FTP dla komputera Mary

### Krok 1: Dostęp do dokumentu tekstowego na laptopie Mary.

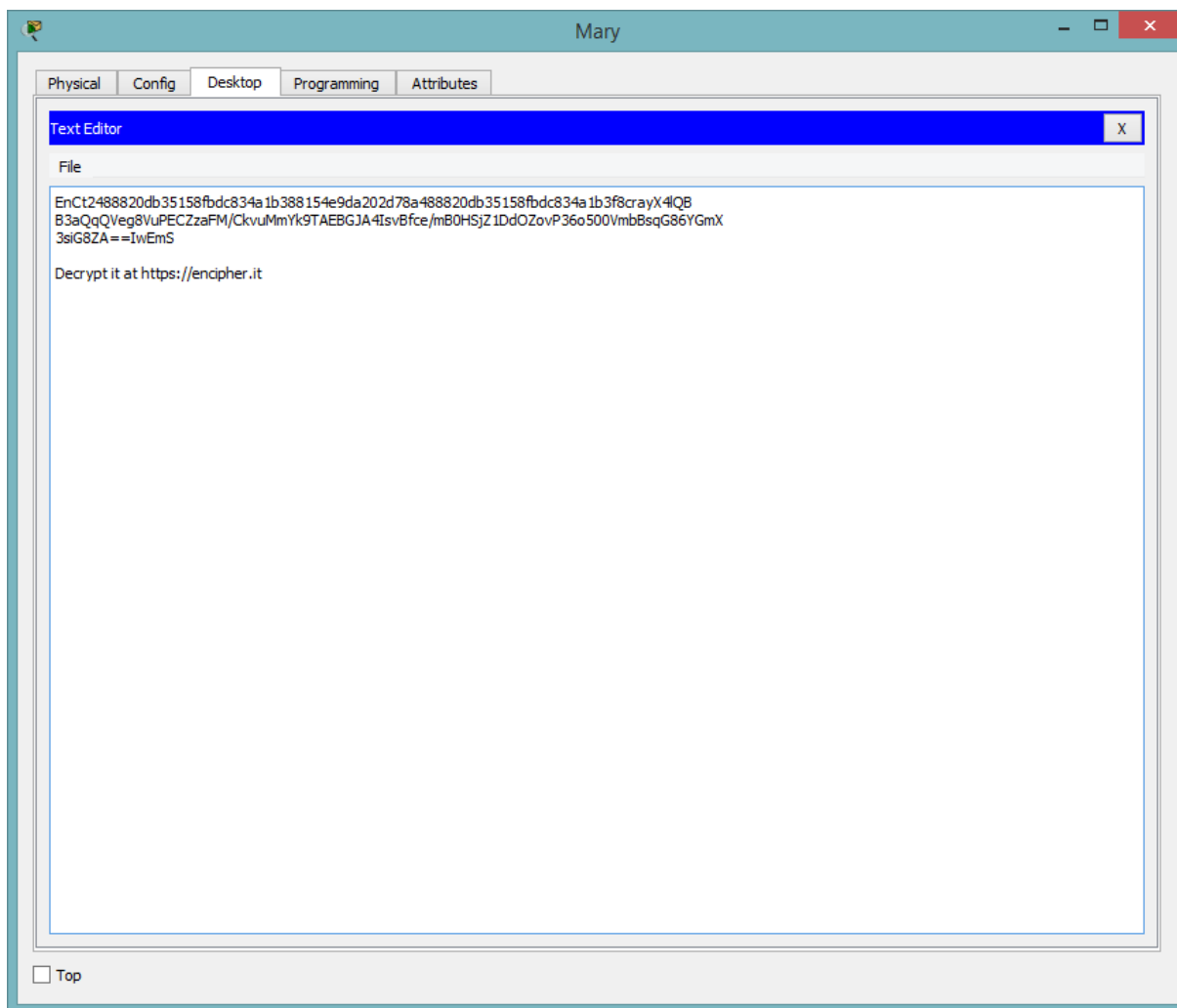
W Healthcare at Home wybierz laptop Mary i odszukaj plik tekstowy o nazwie **ftplogin.txt**.



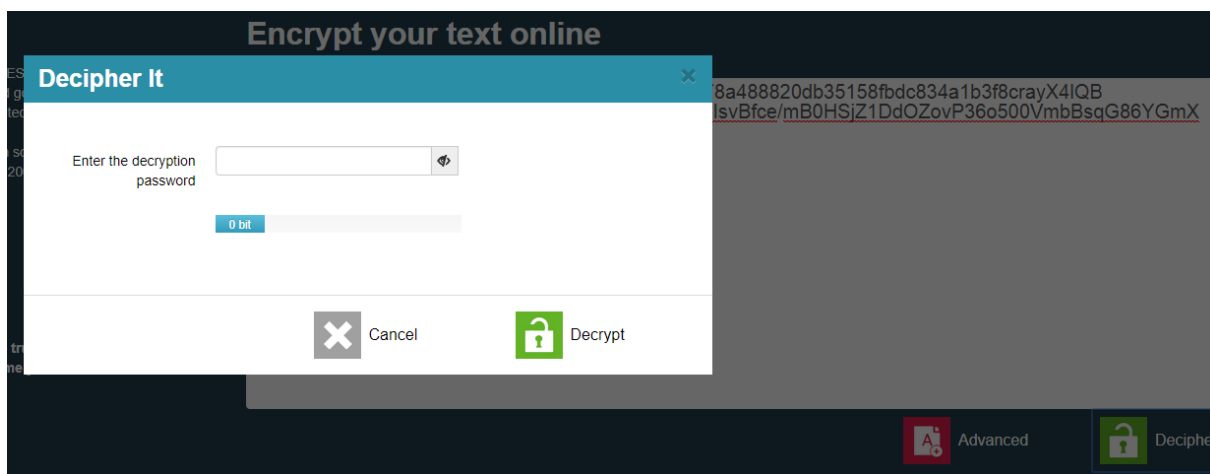
## Krok 2: Odszyfruj informacje o koncie FTP Mary.

Pytanie: Czy zaszyfrowana wiadomość ujawnia tekst jawny? Czy można coś z niej odczytać?

Mary pozostawiła informację o stronie szyfrującej w swoim pliku txt. Przejdź do strony i odszyfruj zaszyfrowaną wiadomość.



Patrząc na zaszyfrowaną wiadomość nie da się niestety nic odczytać ale Mary zostawiła wskazówkę.



Nie ma możliwości odszyfrować wiadomości bez podania hasła.

## Krok 2a: Odgadnij hasło użytkownika

Pytanie: Jaka metoda szyfrowania została wykorzystana? Dlaczego wymagany jest klucz? W jaki sposób możesz pozyskać klucz?  
Załóżmy, że Mary stosuje podstawowe metody zabezpieczeń konta.

1. Unikalne hasło dla nowego konta
2. Minimum 8 znaków
3. W kombinacja musi się być minimum jedna cyfra

Pytanie: Jakie inne podstawowe zasady tworzenia haseł są Tobie znane?

Biorąc pod uwagę powyższe informacje sprawdź:

mary1234, 1234mary, password1, passwordftp, maryftp1, maryftp12, maryftp123, 123maryftp, ftpmary123, i inne kombinacje jakie przychodzą Ci na myśl.

Jakie hasło do zaszyfrowania wykorzystała Mary? Jakie dane logowania do serwera FTP posiada Mary?


### Encrypt your text online


Account Information:


Mary

Username= mary

Password= cisco321

 Decrypt file

 Advanced

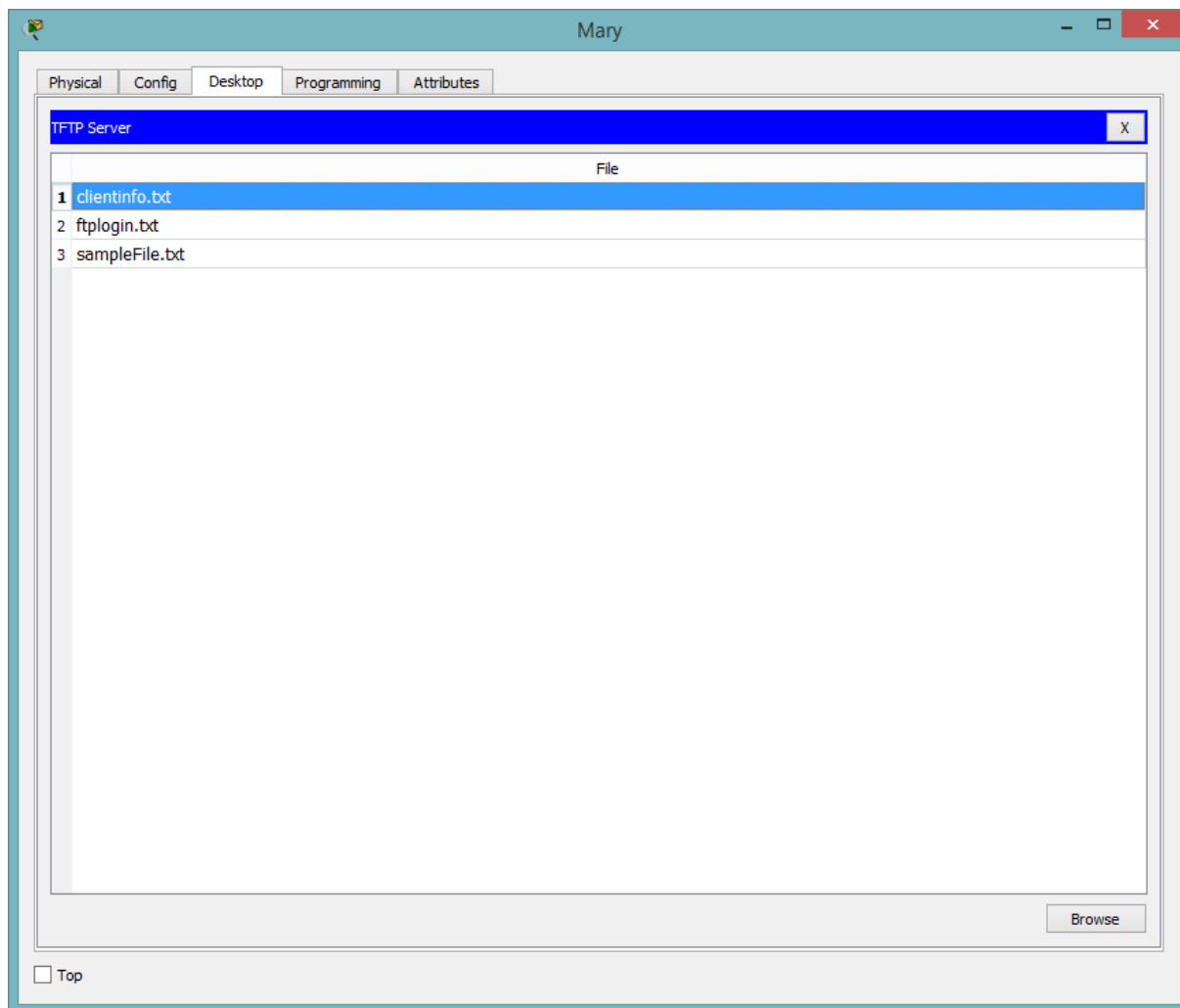
 Encipher It

Mary wykorzystała 18 bitowe szyfrowanie. Klucz jest wymagany aby nieautoryzowany użytkownik nie miał możliwości dostać się do zaszyfrowanego pliku. Pozyskanie klucza jest metodą pracochłonną. Nie zawsze się uda. W tym przypadku Mary do odszyfrowania pliku miała hasło: maryftp123. Po jego wpisaniu pojawia nam się okno, który widać wyżej. Mamy już dane do logowania na FTP.

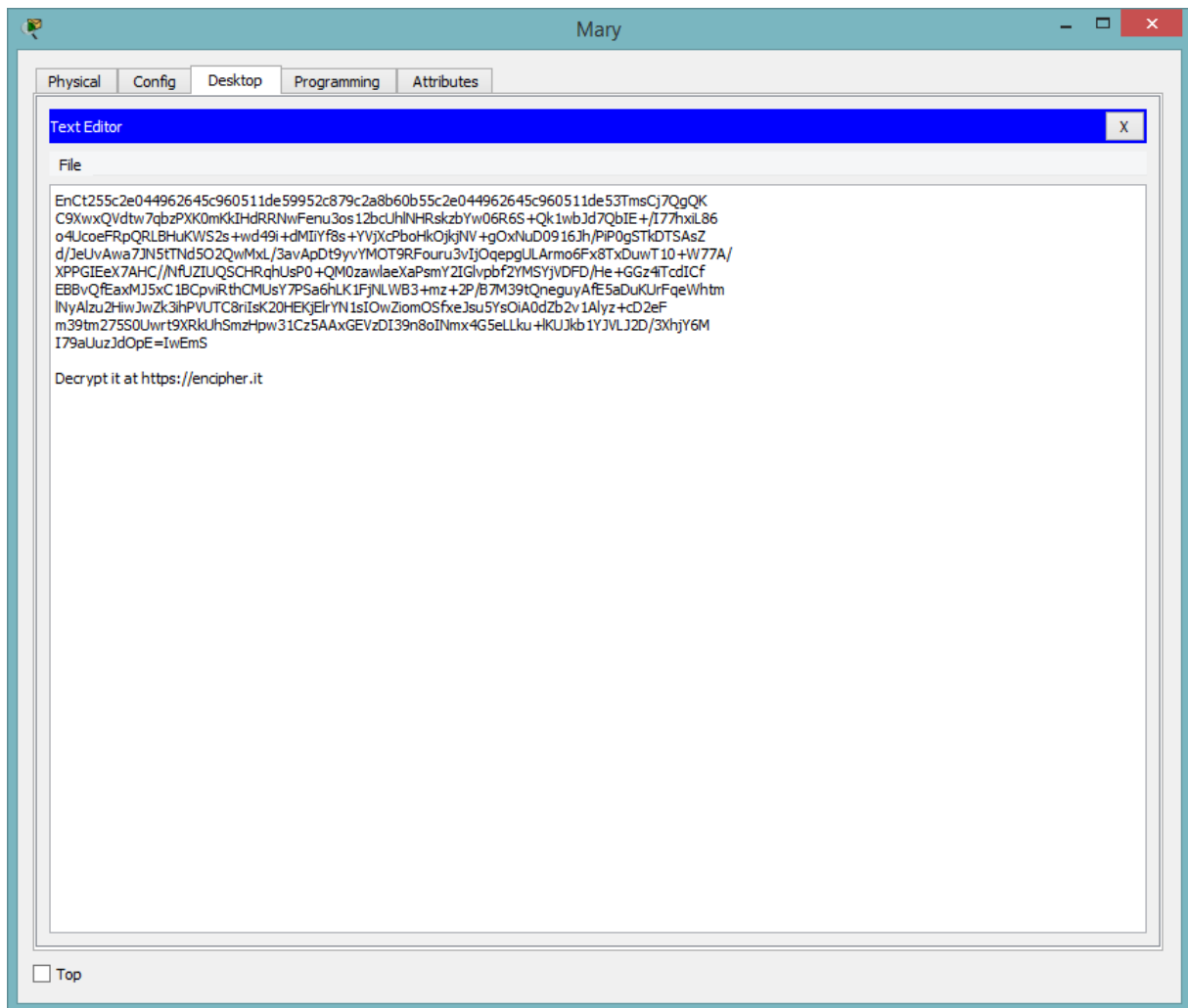
## Część 2: Wyślij poufne dane wykorzystując FTP

### Krok 1: Zobacz dokument poufny na laptopie Mary.

Na laptopie Mary znajdują się inne pliki tekstowe. Który plik (i dlaczego) jest poufny? Czy możesz odczytać zawartość? Czy znasz hasło odszyfrowujące?



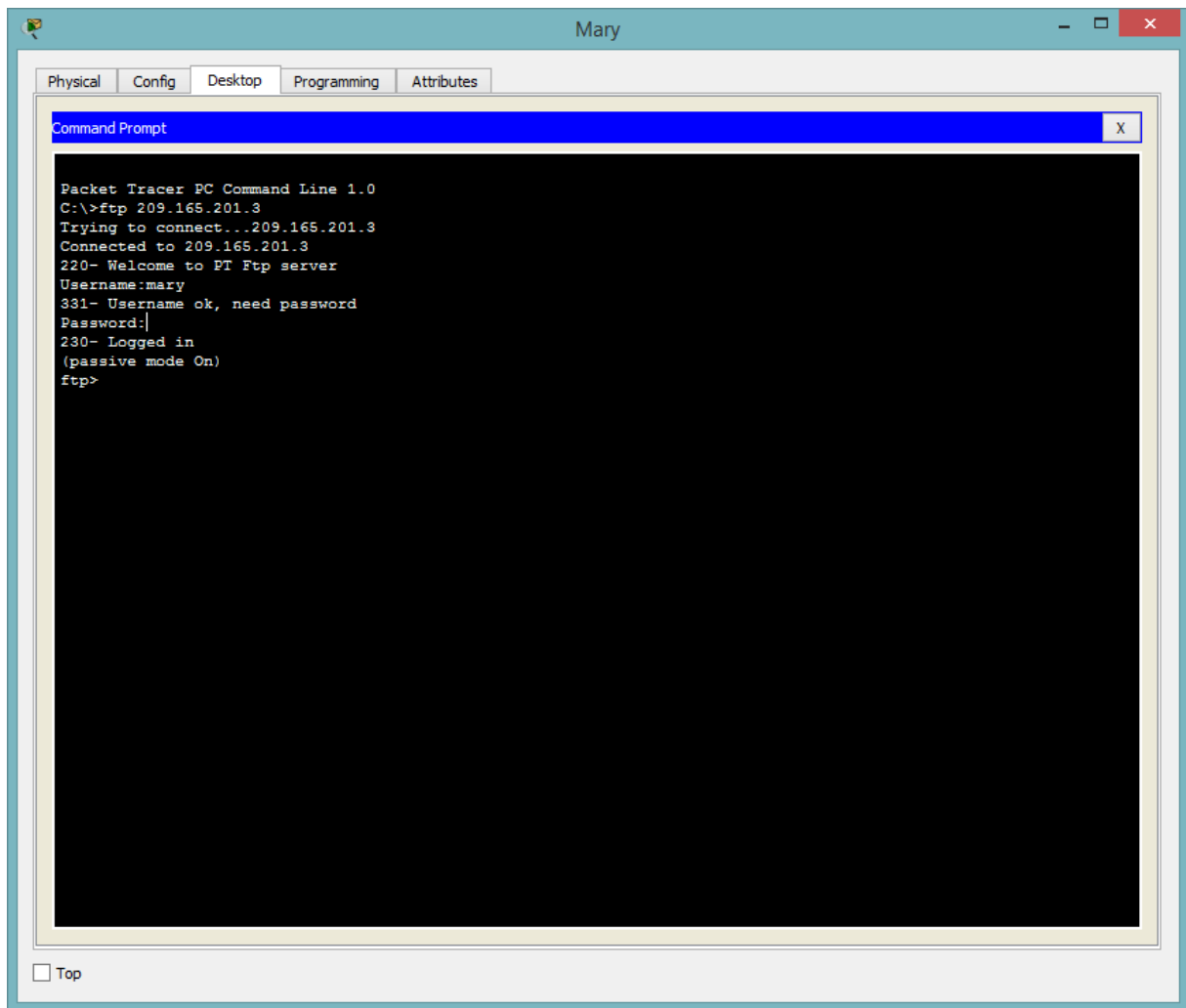
Na laptopie Mary znajduje się inny poufny plik tekstowy o nazwie clientinfo.txt. Plik jest plikiem poufnym ze względu, że znajdują się tam zapewne jak sama nazwa wskazuje dane klienta.



Plik jak w przypadku powyżej jest również zaszyfrowany. Nie mamy możliwości go odczytać bez podania hasła.

## Krok 2: Zdalnie połącz się z serwerem FTP.

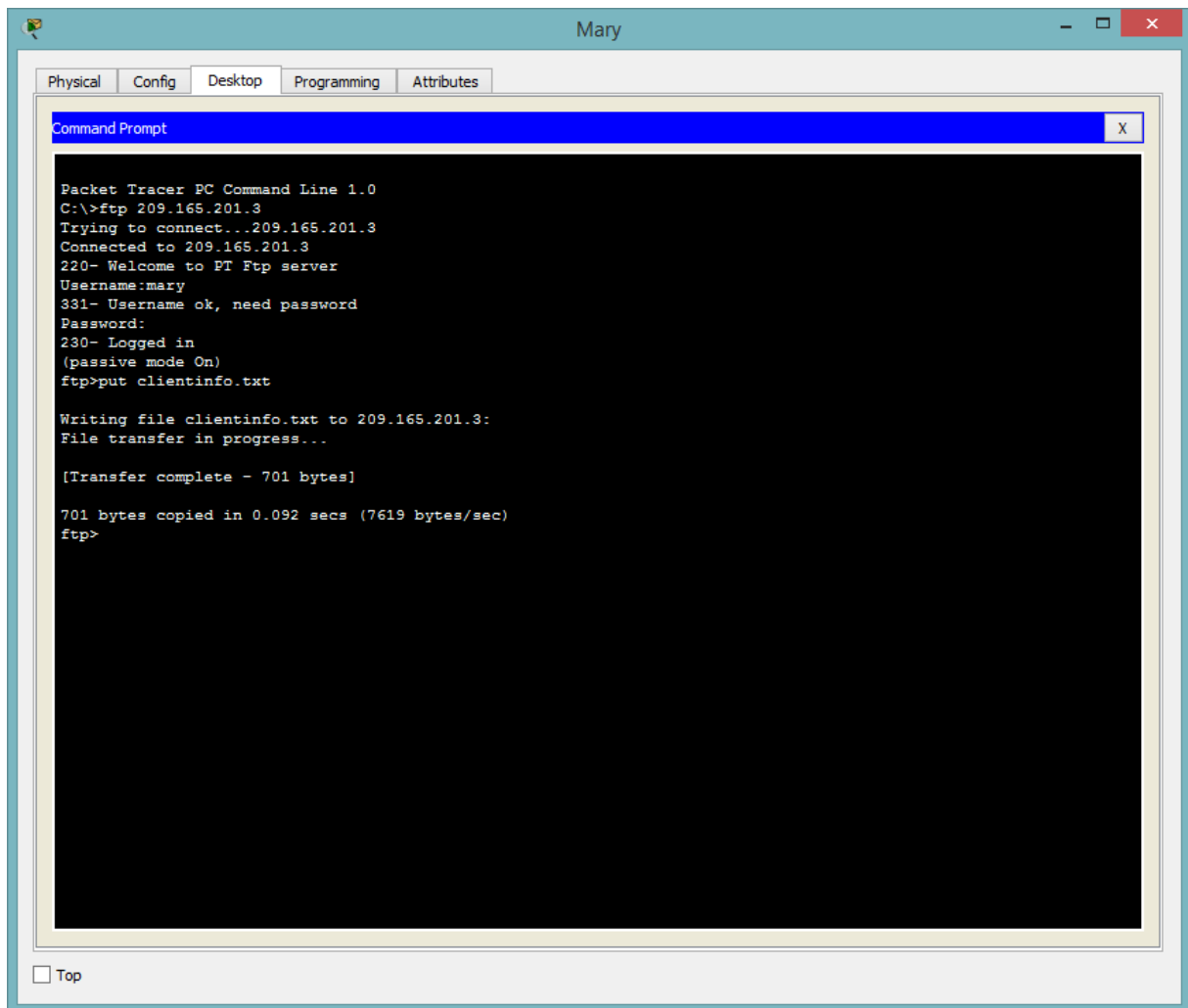
Wykorzystaj **Wiersz poleceń** i komendę **ftp <IP>** aby podłączyć się do serwera **FTP / WWW** w **Metropolis Bank HQ**. Pytanie: Jakiego adresu IP należy użyć to połączenia się z serwerem FTP?



Jak widać połączenie się udało. Aby Mary mogła zalogować się do serwera FTP / WWW w Metropolis Bank HQ musi użyć adresu publicznego ponieważ nie znajduje się w tej sieci. Gdyby się znajdowała w tej samej sieci używałaby adresu prywatnego.

### Krok 3: Prześlij plik na serwer FTP.

Wykorzystaj **Wiersz poleceń i komendę put <file>** w celu umieszczenia plików na serwerze FTP/WWW  
Scenariusz: Osoba podsłuchująca ruch sieciowy przechwyciła plik. Pytanie: Jaką treść zobaczy atakujący?



The screenshot shows a Packet Tracer PC Command Line window titled "Mary". The window has tabs for Physical, Config, Desktop, Programming, and Attributes. The Command Prompt area displays the following text:

```
Packet Tracer PC Command Line 1.0
C:\>ftp 209.165.201.3
Trying to connect...209.165.201.3
Connected to 209.165.201.3
220- Welcome to PT Ftp server
Username:mary
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>put clientinfo.txt

Writing file clientinfo.txt to 209.165.201.3:
File transfer in progress...

[Transfer complete - 701 bytes]

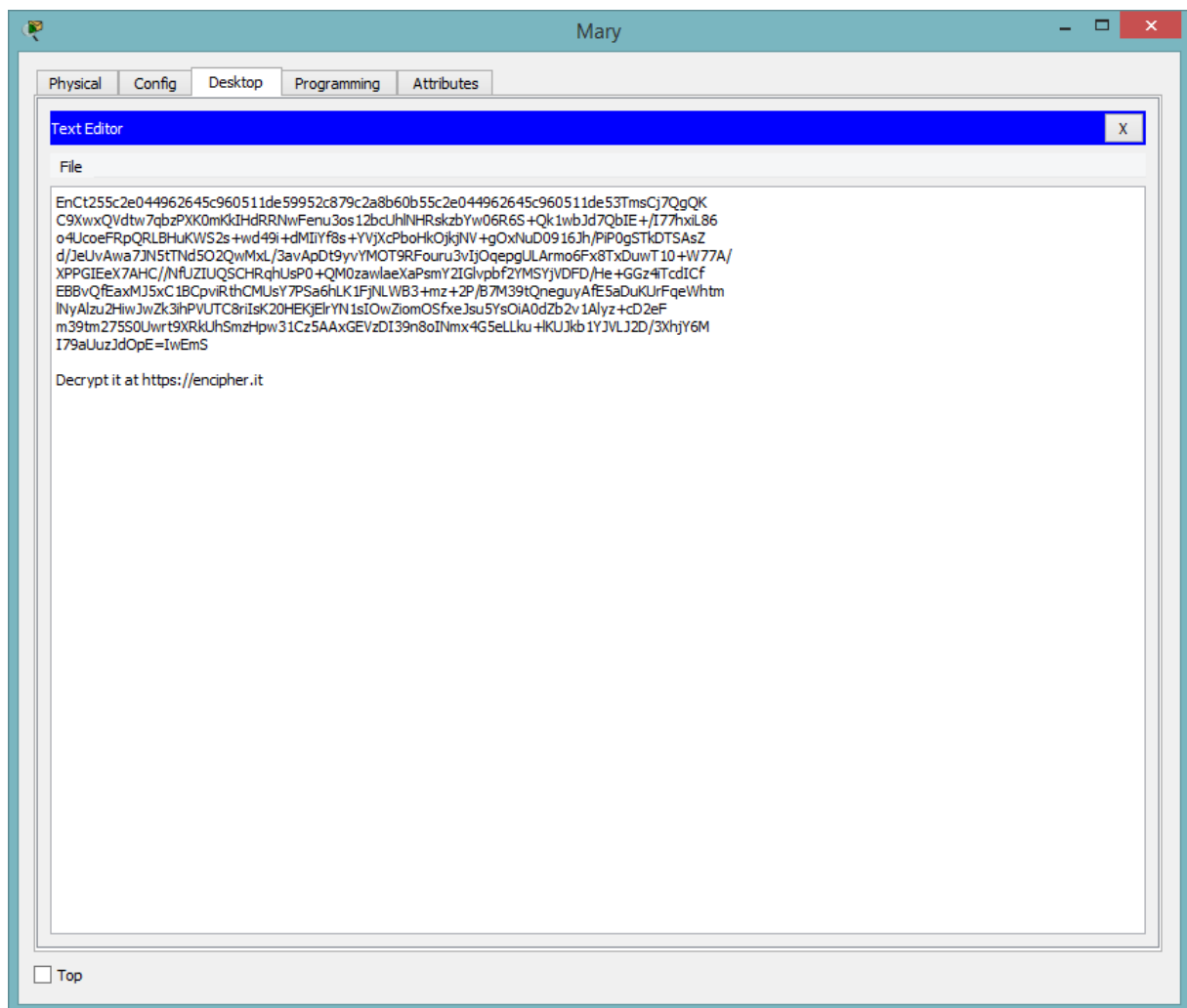
701 bytes copied in 0.092 secs (7619 bytes/sec)
ftp>
```

At the bottom of the window, there is a checkbox labeled "Top" which is currently unchecked.

Jeśli osoba atakująca przechwyciła plik nie jest w stanie nic zrobić ponieważ plik jest zaszyfrowany. Próbuąc go rozszyfrować potrzebuje znać hasło.



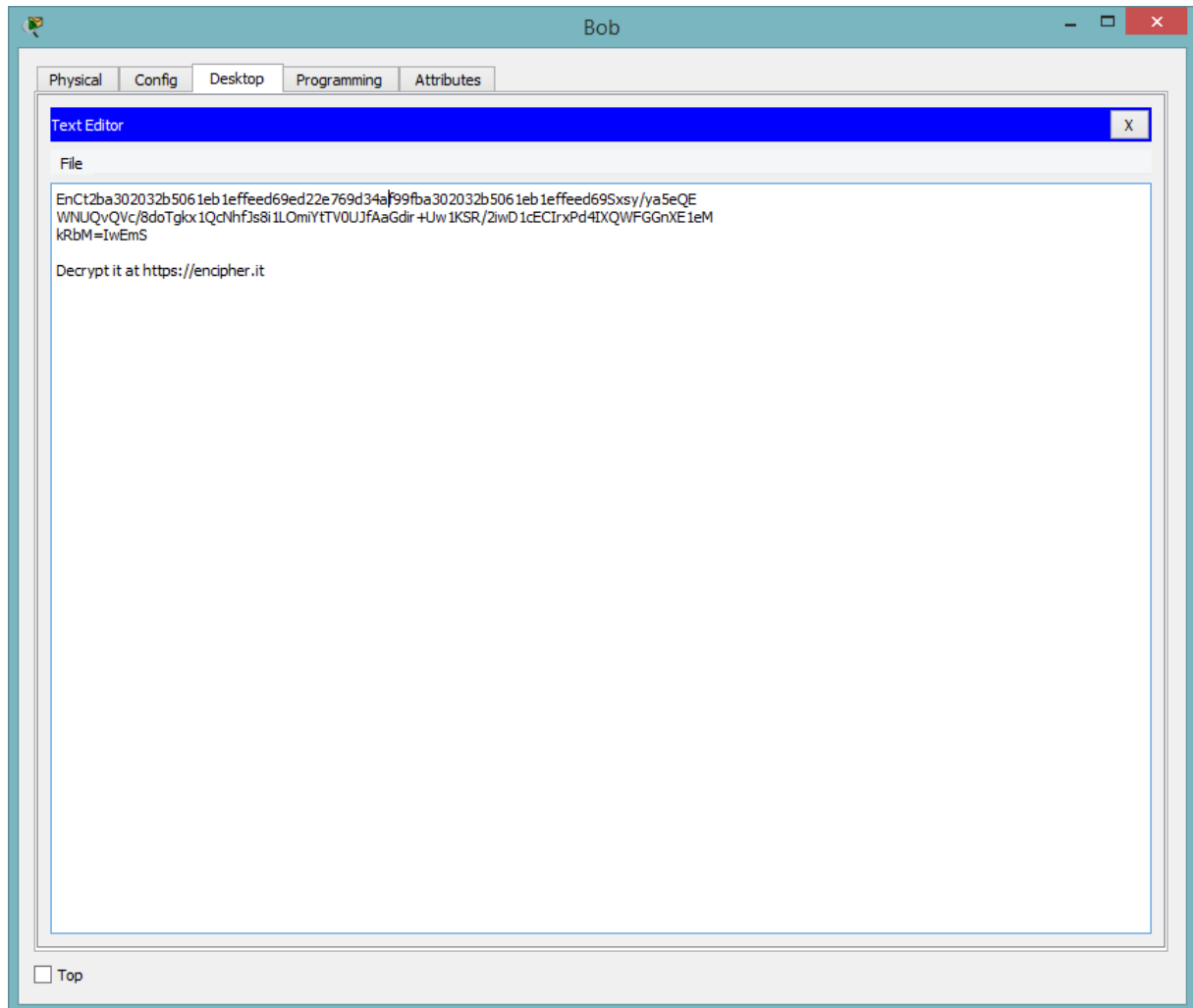
Atakujący zobaczy:



### Część 3: Zlokalizuj dane logowania na konto FTP dla komputera Boba.

#### Krok 1: Otwórz dokument tekstowy na komputerze Boba.

Postępuj analogicznie jak w części 1 aby odszukać plik tekstowy na komputerze Boba.



## Krok 2: Odszyfruj informacje o koncie FTP Boba.

Postępuj analogicznie jak w części 1 aby odszyfrować informacje o koncie Boba. Pytanie: Jakie hasło do zaszyfrowania wykorzystał Bob? Jakie dane logowania do serwera FTP posiada Bob?

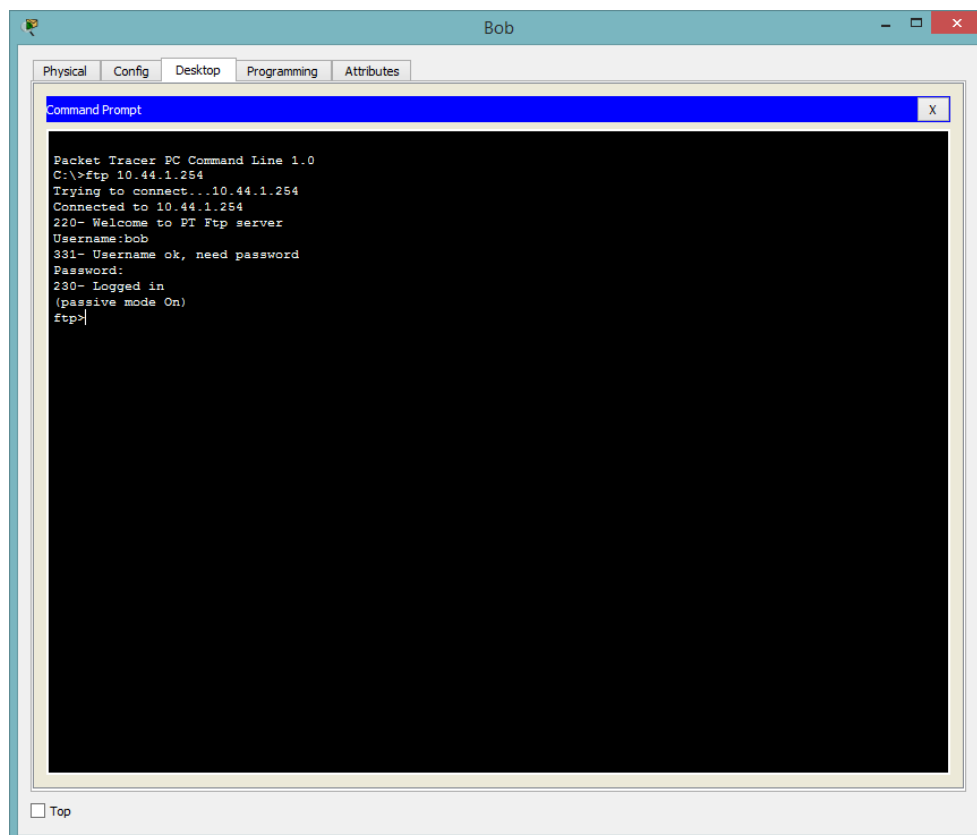


Bob wykorzystał hasło 26 bitowe i jest to: bobftp123 czyli analogicznie do mary. Bob posiada dane do logowania jak na screenie powyżej.

## Część 4: Pobierz poufne dane przy użyciu FTP

### Krok 1: Zdalnie połącz się z serwerem FTP.

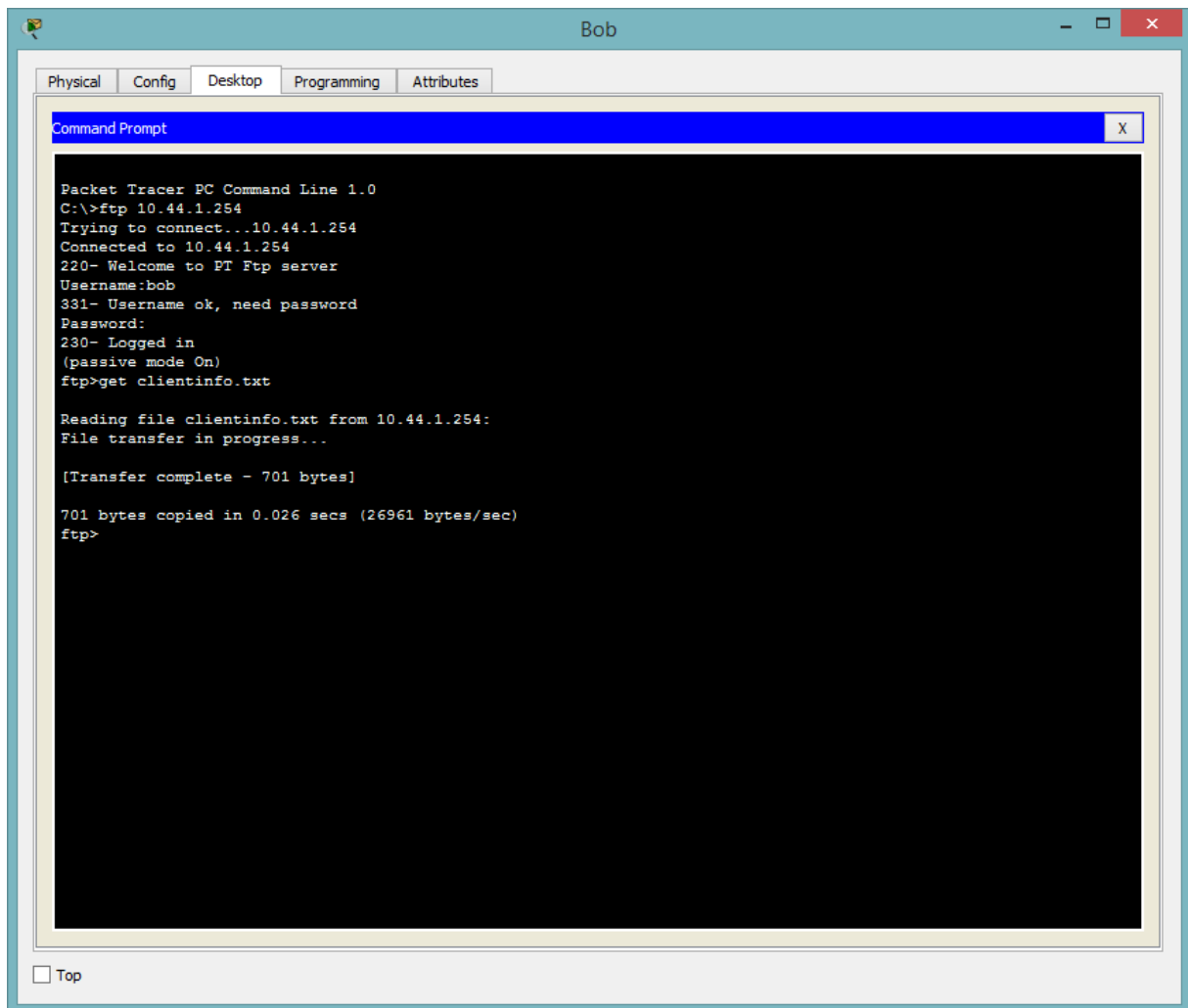
Analogicznie jak poprzednio połącz się z serwerem FTP. Jaki adres należy wybrać do połączenia?



W tym przypadku trzeba użyć adres prywatnego ponieważ bob znajduje się w sieci Metropolis Bank HQ. Adres 10.44.1.254

## Krok 2: Pobierz plik do komputera Boba.

Korzystając z komendy **get <file>** pobierz plik **clientinfo.txt**. Czy znasz już hasło do odszyfrowania wiadomości? Jeśli nie udało Ci się odgadnąć jeszcze hasło wypisz hasła (minimum 10) jakie przychodzą Ci do głowy, czasem odpowiedź mamy dosłownie „przed sobą”... Jeśli się nie uda przejdź do części 5.



```
Bob
Physical Config Desktop Programming Attributes
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ftp 10.44.1.254
Trying to connect...10.44.1.254
Connected to 10.44.1.254
220- Welcome to PT Ftp server
Username:bob
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>get clientinfo.txt

Reading file clientinfo.txt from 10.44.1.254:
File transfer in progress...

[Transfer complete - 701 bytes]

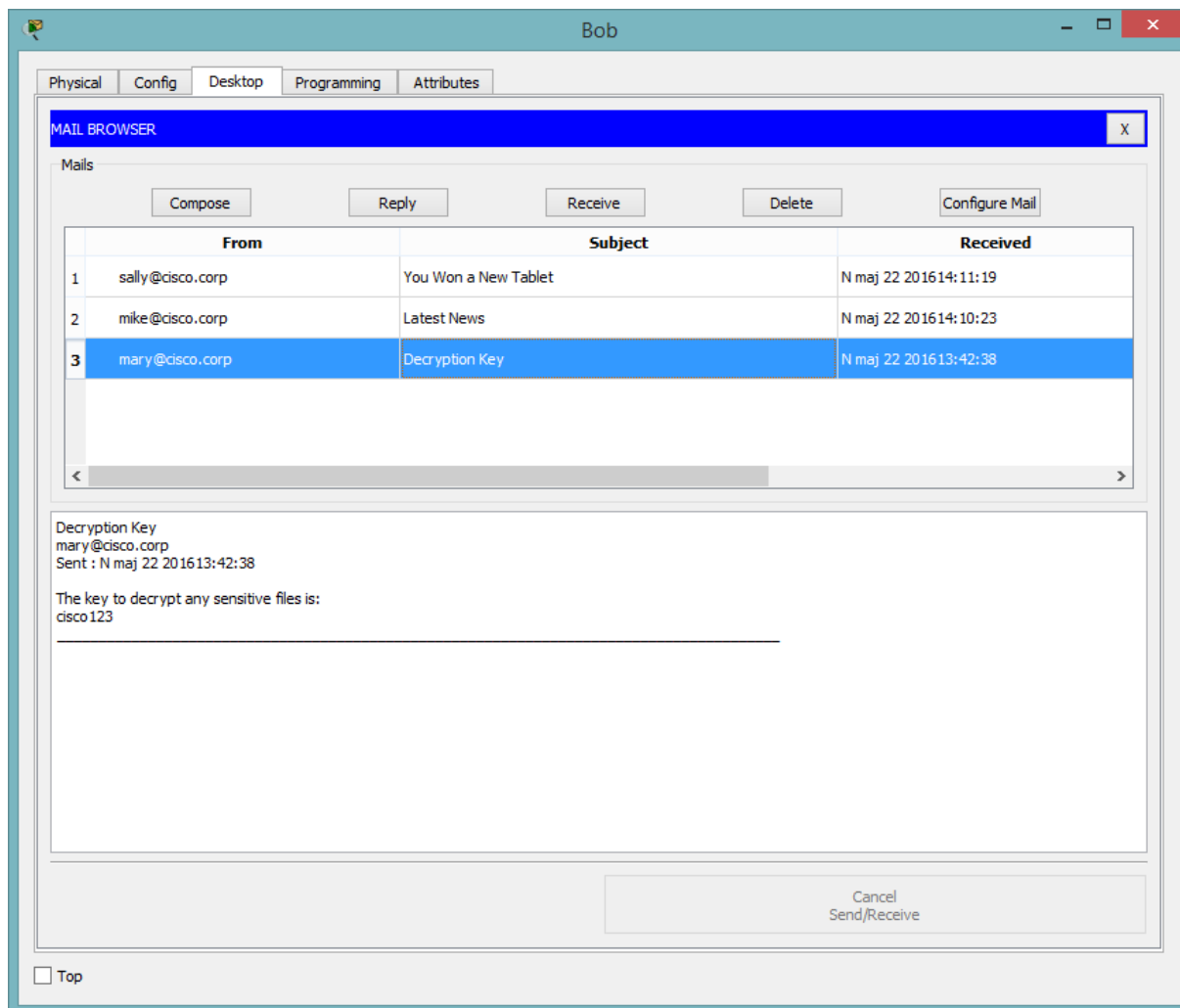
701 bytes copied in 0.026 secs (26961 bytes/sec)
ftp>
```

Za pierwszym razem udało się uzyskać dostęp. Hasło to cisco123.

## Część 5: Odszyfruj zawartość pliku clientinfo.txt

### Krok 1: Odszukaj klucz deszyfrujący.

Masz dostęp do komputera Boba który znajduje się w sieci Metropolis Bank HQ. Pytanie: Co warto sprawdzić w celu poszukiwania klucza? Sprawdzając mail pamiętaj o przyciskach funkcyjnych w symulacji PT.




Po sprawdzeniu maila okazuje się, że Mary wysłała klucz Bobowi.


## Krok 2: Odszyfruj zawartość pliku clientinfo.txt.


### Encrypt your text online

Name|Zip Code|Credit Card

Plato X. Riggs|2769|5537342697671706  
Drew N. Stark|40008|532605 072104 7364  
Laith Wilkerson|21800|516234 6483327961  
Drew A. Dennis|33024|4716904313886  
Genevieve Robertson|25498|491 65497 20952 457  
Paki Parsons|419043|492954 7171363013  
Teagan N. Avery|64416|4485 5676 5330 3713  
Joy B. Goodman|6048TB|419978 0389706805  
Orla L. Rowe|93081|520 88110 11661 765  
Wynter English|1396|534047 781153 0565

 Decrypt file

 Advanced

 Encipher It

Udało się odszyfrować plik.

Udało mi się wykonać wszystkie punkty poprawnie co pokazuje:

Activity Results

Time Elapsed: 01:04:27

Congratulations Guest! You completed the activity.

Overall Feedback | Assessment Items | Connectivity Tests

Congratulations! You successfully completed the Packet Tracer File and Data Encryption activity. However, your final score may change based on your answers to the questions in the Instructions. Consult your instructor.