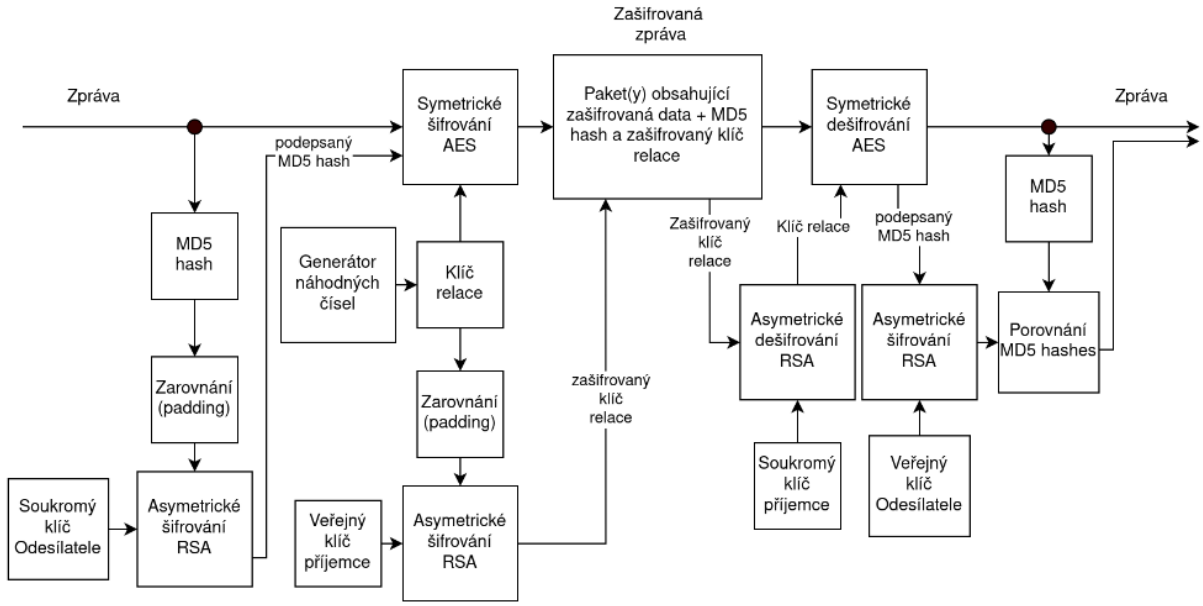
VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA INFORMAČNÍCH TECHNOLOGIÍ


# Kryptografie 2. Projekt 2023 / 24

Bc. Petr Pouč - xpoucp01

11. dubna 2023

Cílem projektu bylo vytvořit hybridní šifrování pro komunikaci mezi klientem a serverem. Při implementaci hybridního šifrování byly použity algoritmy AES 128 bit, RSA 2048 a MD5 hash.




Obrázek 1: Schéma implementovaného hybridního šifrování

## Vytvoření klíčů

Pro symetrickou kryptografii se používá funkce `generate_session_key()`, která vytváří náhodný 128 bitový klíč pomocí funkce `get_random_bytes()`.

Pro asymetrickou kryptografii se používají klíče RSA. Generování klíčů probíhá ve funkci `generate_rsa_keys()`. Klíče jsou následně uloženy jako cert/id_rsa (soukromý klíč) a cert/id_rsa.pub (veřejný klíč).

Symetrický klíč (klíč relace) se používá k šifrování zpráv AES v režimu EAX. Je generován při každé nové komunikaci mezi klientem a serverem a následně je šifrován RSA veřejným klíčem příjemce a poslán serveru.

Asymetrické klíče jsou použity pro šifrování a dešifrování symetrického klíče použitého pro šifrování zpráv. Veřejný klíč je použit klientem k šifrování symetrického klíče a soukromý klíč je použit serverem k dešifrování symetrického klíče.

Dále je použit soukromý klíč použit k asymetrickému zašifrování MD5 hashe.

## Padding

K vyplnění velikosti bloku šifrovacího algoritmu jsem implementoval vlastní padding na principu OAEP. Padding se aplikuje na hash před tím, než je přidán do zprávy tak, aby se délka hashe rovnala velikosti bloku použitého šifrovacího algoritmu. Já hash doplňuji nulami, aby se jeho délka rovnala 16-ti bajtům.

## Zajištění integrity

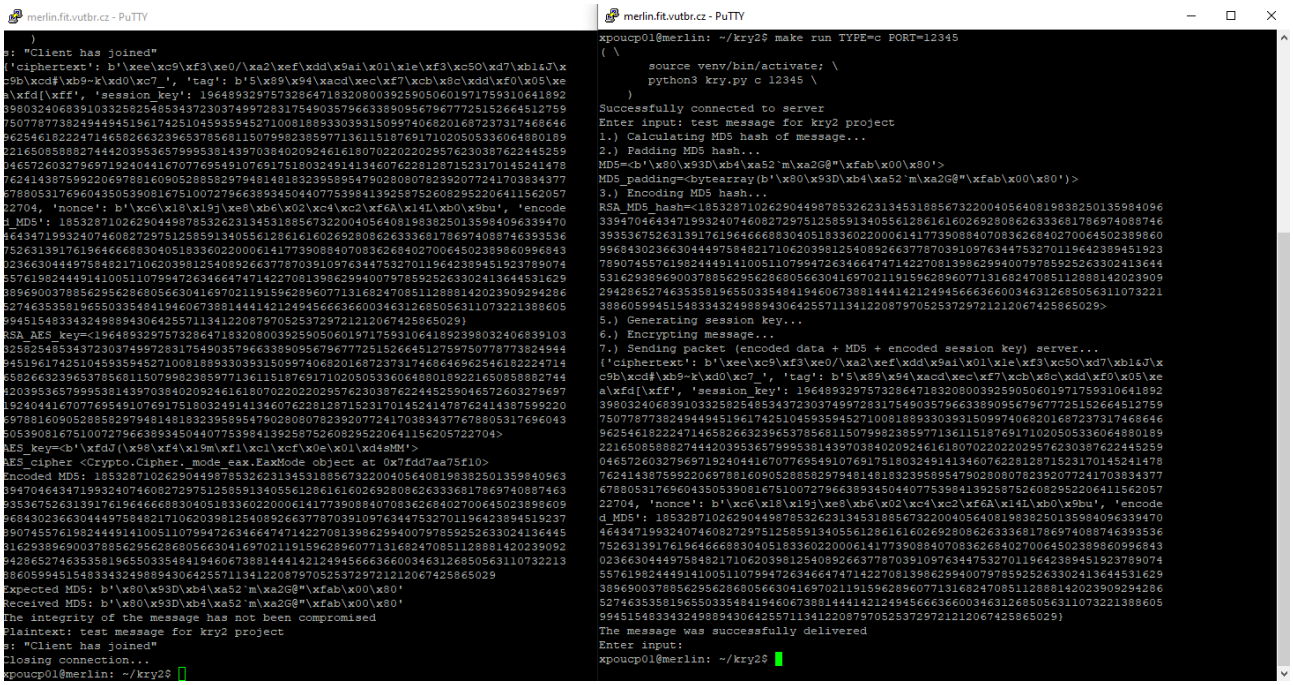
Pro zajištění integrity je k odeslané zprávě přidán asymetricky šifrovaný MD5 hash. Ten je dále spolu s klíčem relace a zprávou symetricky šifrován AES šifrou.

Po příjmu zprávy je použit soukromý klíč příjemce k dešifrování klíče pro symetrickou šifru AES (klíče relace). Pomocí něj je následně provedeno dešifrování paketu, který byl šifrován pomocí AES. Z něj lze získat podepsaný MD5 hash, který nám pomůže určit zachování integrity zprávy. Pokud se získaný MD5 hash rovná zakódovanému MD5 hashi zprávy, zpráva je považována za platnou.

```
Expected MD5: b'\xaa\xc7\xd5m\xf75S\xfe\xe6VM\xd8\x9d\xda\xa4\xc8'
Received MD5: b'\xaa\xc7\xd5m\xf75S\xfe\xe6VM\xd8\x9d\xda\xa4\xc8'
The integrity of the message has not been compromised
Plaintext: Testing message for KRY2 project
```

Obrázek 2: Zajištění integrity pomocí podepsaného MD5 hashe

K šifrovování a dešifrování pomocí algoritmu RSA jse použil funkce `_encrypt` a `_decrypt` z modulu RSA.




Obrázek 3: Zajištění integrity pomocí podepsaného MD5 hashe

## Zhodnocení bezpečnosti

Bezpečnost tohoto hybridního šifrování by mohla být ohrožena, pokud by útočník získal přístup k soukromému klíči. Délka klíče je 128 bitů pro AES a 2048 bitů pro RSA. Tyto délky jsou obecně považovány za dostatečně bezpečné a jsou běžně používány v moderní kryprografii.