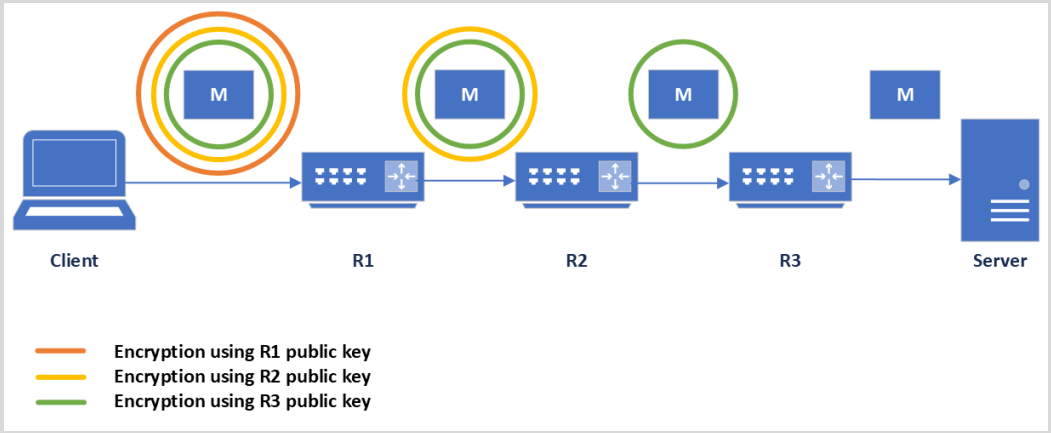
The Onion Routing: Question 5 A

- Imagine an onion routing scenario with 3 routers as displayed in the figure
- For simplification, the message from the client which consists of ASCII characters is first encoded as hexadecimal numbers and each character is encrypted separately using RSA
- Public keys
  - R2: e=809, n=4189
  - R3: e=511, n=851
- Message that R2 received from R1
  - ['0xf09', '0x17e', '0x2ab', '0xbbe', '0xcc6', '0x1050', '0x1050', '0xf14', '0x38c', '0xd62', '0xd57', '0xd57', '0x2b', '0x2b', '0x2b', '0x36e', '0xe0c', '0x816', '0x1050', '0x36e', '0xd19', '0xf65', '0xd57', '0x564', '0xdc6', '0xf64', '0xece', '0x103a', '0xe57', '0x8bd']



The Onion Routing: Question 5 A

- Organizational
  - You will be divided into two groups – R2 and R3
    - Students from group R2 will simulate router R2 and students from group R3 will simulate router R3
  - You will receive the private RSA keys for R2/R3 router by email
  - Form pairs – one person from group R2, one from group R3
    - You can use the course forum in ILIAS to find your partner
  - R2 group task
    - Decrypt the message from R1 (previous slide) and send it to your partner from group R3
    - You can share the decrypted message with more students from group R3 if they couldn't find a partner
  - R3 group task
    - Decrypt the message that you received from your partner from group R2 and encode it into ASCII characters
    - You should get a meaningful message in the form "GET <URL>"

The Onion Routing: Question 5 A

- You can use whatever tools you want – pen and paper, calculator, programming language, online tools, …
- Submissions
  - Submit the result of your decryption
  - Describe how you got the result and which tool you used, submit your source code if applicable
  - Deadlines
    - Group R2: **Thursday 26.5. 18:00** (the deadline for the other questions remains unchanged, i.e., 29.5.)
    - Group R3: **Sunday 29.5. 18:00** (the same as for the rest of the questions)
  - If you are a member of group R3 and you haven't received the message from your partner from group R2 (or the message is incorrect), you can still get full points if you submit your solution using the message from R1 as your input instead

The Onion Routing: Question 5 B

- The encryption scheme in question 5 A isn’t particularly secure. What are its weaknesses? How would you make it more secure?